JUN 27 1986

Y 1.1/8:99-647

99TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
99-647

COMPLETED /// ORIGINAL

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

JUNE 19, 1986.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. KASTENMEIER, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany H.R. 4952]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4952) to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception".

(C) by striking out "as a common carrier" and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

61-068 O

COD

(B) by inserting ", electronic," after "wire".

(4) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(5) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title);

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(2) Section 2511(2)(f) of title 18, United States Code, is amended—

(A) by inserting "or chapter 121" after "this chapter"; and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(3) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted—

"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

"(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

"(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

"(IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communications Act of 1934; or

"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled encrypted.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register (as that term is defined for the purposes of chapter 206 (relating to pen registers) of this title);

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

"(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted.".

(c) Technical and Conforming Amendments.—(1) Chapter 119 of title 18, United States Code, is amended—

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2516(1) and 2518(10)), by striking out "wire or oral" each place it appears (including in any section heading) and inserting "wire, oral, or electronic" in lieu thereof; and

(B) in section 2511(2)(b), by inserting "or electronic" after "wire".

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "**and electronic communications**" after "**wire**".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "and electronic communications" after "Wire".

(4) Section 2510(5)(a) of title 18, United States Code, is amended by striking out "communications common carrier" and inserting "provider of wire or electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "any communication common carrier" and inserting "a provider of wire or electronic communication service" in lieu thereof;

(B) by striking out "of the carrier of such communication" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": *Provided*, That said communication common carriers" and inserting ", except that a provider of wire communication service to the public" in lieu thereof.

(6) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "communication common carriers" and inserting "providers of wire or electronic communication service" in lieu thereof;

(B) by striking out "communication common carrier" each place it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(C) by striking out "if the common carrier" and inserting "if such provider" in lieu thereof.

(7) Section 2512(2)(a) of title 18, United States Code, is amended—

(A) by striking out "a communications common carrier" the first place it appears and inserting "a provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended by striking out "communication common carrier" and inserting "provider of electronic communication service" in lieu thereof.

(d) Penalties Modification.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:

"(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

"(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

"(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

"(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

"(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.".

(e) Exclusivity of Remedies with Respect to Electronic Communications.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:

"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.".

SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(B) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

"(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) In General.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) Relief.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) Computation of Damages.—The court may assess as damages in an action under this section whichever is the greater of—

"(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) Defense.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

"(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) Wire and Oral Interceptions.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),";

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),"; and

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations)";

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

"(i) the location of any fugitive from justice from an offense described in this section; or"; and

(4) by redesignating paragraph (h) as paragraph (j).

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516 of title 18 of the United States Code is amended by adding at the end the following:

"(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.".

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of the United States Code is amended by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance".

(c) COMMENCEMENT OF 30-DAY PERIOD AND POSTPONEMENT OF MINIMIZATION.—Section 2518(5) of title 18 of the United States Code is amended—

(1) by inserting after the first sentence the following: "Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered."; and

(2) by adding at the end the following: "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.".

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii) of title of the United States Code is amended by inserting "except as provided in subsection (11)," before "a particular description".

(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(i) in the case of an application with respect to the interception of an oral communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(III) the judge finds that such specification is not practical; and

"(ii) in the case of an application with respect to a wire or electronic communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(III) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.".

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".

SEC. 107. INTELLIGENCE ACTIVITIES.

(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3117. Mobile tracking devices

"(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

"(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices.".

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States Code, is amended—

(1) by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;

(2) by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and

(3) by adding at the end the following:

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.".

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§ 2521. Injunction against illegal interception

"Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.".

(b) Clerical Amendment.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

"2521. Injunction against illegal interception.".

SEC. 111. EFFECTIVE DATE.

(a) In General.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) Special Rule for State Authorizations of Interceptions.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

(2) the date two years after the date of the enactment of this Act.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

"CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

"Sec.
"2701. Unlawful access to stored communications.
"2702. Disclosure of contents.
"2703. Requirements for governmental access.
"2704. Backup preservation.
"2705. Delayed notice.
"2706. Cost reimbursement.
"2707. Civil action.
"2708. Exclusivity of remedies.
"2709. Counterintelligence access to telephone toll and transactional records.
"2710. Definitions.

"§ 2701. Unlawful access to stored communications

"(a) Offense.—Except as provided in subsection (c) of this section whoever—

"(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

"(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

"(b) Punishment.—The punishment for an offense under subsection (a) of this section is—

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

"(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

"(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—

"(1) by the person or entity providing a wire or electronic communications service;

"(2) by a user of that service with respect to a communication of or intended for that user; or

"(3) in section 2703 or 2704 of this title.

"§ 2702. Disclosure of contents

"(a) Prohibitions.—Except as provided in subsection (b)—

"(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

"(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(b) Exceptions.—A person or entity may divulge the contents of a communication—

"(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

"(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

"(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

"(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

"(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

"(6) to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime.

"§ 2703. Requirements for governmental access

"(a) Contents of Electronic Communications in Electronic Storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

"(b) Contents of Electronic Communications in a Remote Computing Service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

"(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

"(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

"(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(c) RECORDS CONCERNING ELECTRONIC COMMUNICATIONS SERVICE OR REMOTE COMPUTING SERVICE.—A governmental entity may require a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

"(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

"(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(3) obtains a court order for such disclosure under subsection (d) of this section.

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

"§ 2704. Backup preservation

"(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

"(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

"(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

"(B) has not initiated proceedings to challenge the request of the governmental entity.

"(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

"(b) Customer Challenges.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

"(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

"(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

"(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning given that term in the Federal Rules of Civil Procedure.

"(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

"(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

"(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

"§ 2705. Delayed notice

"(a) Delay of Notification.—(1) A governmental entity acting under section 2703(b) of this title may—

"(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days; if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

"(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

"(2) An adverse result for the purposes of paragraph (1) of this subsection is—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

"(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

"(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

"(A) states with reasonable specificity the nature of the law enforcement inquiry; and

"(B) informs such customer or subscriber—

"(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

"(ii) that notification of such customer or subscriber was delayed;

"(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

"(iv) which provision of this chapter allowed such delay.

"(6) As used in this subsection, the term 'supervisory official' means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

"(b) Preclusion of Notice to Subject of Governmental Access.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

"(1) endangering the life or physical safety of an individual;

"(2) flight from prosecution;

"(3) destruction of or tampering with evidence;

"(4) intimidation of potential witnesses; or

"(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"§ 2706. Cost reimbursement

"(a) Payment.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) Amount.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

"§ 2707. Civil action

"(a) Cause of Action.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

"§ 2708. Exclusivity of remedies

"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

"§ 2709. Counterintelligence access to telephone toll and transactional records

"(a) DUTY TO PROVIDE.—A Communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

"(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(c) PROHIBITION OF CERTAIN DISCLOSURE.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

"(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

"(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

"§ 2710. Definitions for chapter

"As used in this chapter—

"(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

"(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.".

(b) Clerical Amendment.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access .... 2701".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

SEC. 301. TITLE 18 AMENDMENT.

(a) In General.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS

"Sec.
"3121. General prohibition on pen register use; exception.
"3122. Application for an order for a pen register.
"3123. Issuance of an order for a pen register.
"3124. Assistance in installation and use of a pen register.
"3125. Reports concerning pen registers.
"3126. Definitions for chapter.

"§ 3121. General prohibition on pen register use; exception

"(a) In General.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) Exception.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent or the user of that service.

"(c) Penalty.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register

"(a) Application.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) Contents of Application.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

"§ 3123. Issuance of an order for a pen register

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

"(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER.—An order authorizing or approving the installation and use of a pen register shall direct that—

"(1) the order be sealed until otherwise ordered by the court; and

"(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

"§ 3124. Assistance in installation and use of a pen register

"(a) IN GENERAL.—Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) COMPENSATION.—A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"§ 3125. Reports concerning pen registers

"The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the term 'communications common carrier' has the meaning set forth for the term 'common carrier' in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

"(2) the term 'wire communication' has the meaning set forth for such term in section 2510 of this title;

"(3) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

"(4) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) Clerical Amendment.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers .... 3121".

SEC. 302. EFFECTIVE DATE.

(a) In General.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) Special Rule for State Authorizations of Interceptions.—Any pen register order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

Purpose

The purpose of the legislation is to amend title 18 of the United States Code to prohibit the interception of certain electronic communications; to provide procedures for interception of electronic communications by federal law enforcement officers; to provide procedures for access to communications records by federal law enforcement officers; to provide procedures for federal law enforcement access to electronically stored communications; and to ease certain procedural requirements for interception of wire communications by federal law enforcement officers.

History

When the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers and effects" protected by the Fourth Amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

The telephone is the most obvious example. Its widespread use made it technologically possible to intercept the communications of citizens without entering homes or other private places. When the issue of government wiretapping first came before the Supreme Court in *Olmstead* v. *United States*, 277 U.S. 438, the Court held that wiretapping did not violate the Fourth Amendment, since there was no searching, no seizure of anything tangible, and no physical trespass.[1]

But the *Olmstead* case is remembered not only for its holding but for the prescient dissent of Mr. Justice Brandeis, who predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security? [2]

Forty years later, the Supreme Court accepted the logic of Justice Brandeis in *Katz* v. *United States*, 389 U.S. 347 (1967), holding that the Fourth Amendment applies to government interception of a telephone conversation. At the same time, the Court extended Fourth Amendment protection to electronic eavesdropping on oral conversations in *Berger* v. *New York*, 388 U.S. 41 (1967).

Congress responded in a comprehensive fashion by authorizing government interception, under carefully subscribed circumstances, in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[3] which has come to be known as the Wiretap Act. That legislation protected two common types of communication—telephone conversations and face-to-face oral communications—against electronic eavesdropping. Specifically, the law barred the interception of wire communications over a common carrier unless an appropriate court order had been obtained.[4] Further, it limited the concept of interception to the "aural acquisition" of the contents of a communication.[5] "Oral communications" were protected only in circumstances where there is a reasonable expectation of privacy.[6]

NATURE OF THE PROBLEM

Although it is still not twenty years old, the Wiretap Act was written in different technological and regulatory era. Communications were almost exclusively in the form of transmission of the human voice over common carrier networks. Moreover, the contents of a traditional telephone call disappeared once the words transmitted were spoken and there were no records kept. Consequently the law primarily protects against the aural interception of the human voice over common carrier networks.

The legislation did not attempt to address the interception of text, digital or machine communication.[7] This statutory framework appears to leave unprotected an important sector of the new communications technologies.

Many communications today are carried on or through systems which are not common carriers. Electronic mail, videotex and similar services are not common carrier services. Under existing law the interception of these services or the disclosure of the contents of messages over these services are probably not regulated or restricted. Moreover, totally private systems are rapidly being developed by private companies for their own use. It is not uncommon for businesses now not to use the local telephone comapny in some instances the long distance companies in the creation of voice and data networks. Since these networks are private they are not covered by existing Federal law. In addition, data is transmitted over tradional telephone services as well as by these services. Since data, unlike the human voice, cannot be aurally intercepted, it is also largely unregulated and unrestricted under present law.

---

[1] Olmstead v. United States, 277 U.S. 438, 464 (1927). *Compare*, Dow Chemical Co. v. United States, — U.S. — (May 19, 1986) (aerial photography by government without a warrant does not violate Fourth Amendment); California v. Ciraolo, — U.S. — (May 19, 1986) (same).

[2] 277 U.S. at 474 (Brandeis, J., dissenting).

[3] 18 U.S.C. 2510 *et seq.* hereinafter "Wiretap Act."

[4] 18 U.S.C. 2511.

[5] 18 U.S.C. 2510.

[6] *Id.*

[7] Sen. Rep. No. 1097, 90th Cong., 2d Sess. 90, hereinafter "1968 Senate Report."

Today, we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago. Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.

In 1984 the Federal government engaged in more telephone surveillance and wiretapping than in any year since 1973.[8] Moreover, according to a recent study by the Office of Technology Assessment, Federal agencies are planning to use or already use radio scanners (20 agencies), cellular telephone interception (6 agencies), tracking devices (15 agencies), pen registers (14 agencies), and electronic mail interceptions (6 agencies).[9]

This increased use of a variety of electronic surveillance devices alone is not cause for alarm. There are instances when a particular electronic surveillance technique is justified in a criminal investigation. Congress has recognized this by permitting—under carefully limited circumstance under the Wiretap Act—the tapping of telephone calls or the bugging of rooms. However, despite efforts by both Congress [10] and the courts,[11] legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.

The statutory deficiency in Title III with respect to non-voice communications has been criticized by commentators, Congressional experts, and most recently by both the General Accounting Office and the Office of Technology Assessment.[12] The danger is eloquently pointed out by Professor Richard Posner (now United States Circuit Court Judge):

---

[8] Administrative Office of the United States Courts, *Report on Application for Orders Authorizing or Approving the Interception of Wire or Oral Communications (Wiretap Report) for the Period January 1, 1984 to December 31, 1984.*

[9] Office of Technology Assessment, U.S. Cong., ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985), hereinafter "OTA Report."

[10] *E.g.*, The Wiretap Act, *supra* note 3; Foreign Intelligence Surveillance Act, 50 U.S.C. 101 *et seq.*; Right to Financial Privacy Act, 12 U.S.C. 3401 *et seq.*

[11] *E.g.*, United States v. Torres, 751 F.2d 875 (7th Cir. 1984), *cert. den'd*, —U.S.—, 105 S.Ct. 1853 (1985). (court has authority to issue warrant permitting video surveillance); Katz v. United States, 389 U.S., 347 (1967), (Fourth Amendment applies to government wiretapping of telephone conversation); Berger v. New York, 388 U.S. 41 (1967) (Fourth Amendment applies to electronic eavesdropping on oral conversation).

[12] *See generally, Electronic Communications Privacy Act of 1985: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong., 1st and 2d Sess., hereinafter "House Hearings." *See also* Burnham, *Experts Study Effect on Law of Latest Electronic Services*, N.Y. Times, Mar. 18, 1985 (reporting on study by ACLU Project on Privacy and Technology).

> In the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality. And the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm.[13]

This legal uncertainty poses potential problems in a number of areas. First, it may unnecessarily discourage potential customers form using such systems, and encourage unauthorized users to obtain access to communications to which they are not party.[14] Lack of clear standards may also expose law enforcement officers to liability [15] and endanger the admissibility of evidence.[16]

But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right.[17] Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.[18] Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.[19]

The Committee believes the bill represents a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.

Telecommunications Technologies Under Current Law

RADIO TELEPHONES

When Congress passed the Wiretap Act in 1968, most telephone calls were transmitted as they always had been—by wire. Other technologies, however, were already on the horizon, an inevitability implicitly recognized by Congress in protecting telephone calls carried "in whole or in part" over wire. 18 U.S.C. 2510. Today, only a minority of telephone calls are made through wire alone; the majority combine wire with some form of radio technology, usually microwave.

a. Microwave

Microwave consists of extremely high frequency radio waves transmitted point-to-point on line-of-sight paths between antennas located on towers or building tops (in terrestrial microwave systems) and between satellites and earth station "dish" antennas (in satellite-based systems). Like most radio transmissions, the microwave portion of a telephone call is vulnerable to interception.[20]

---

[13] Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176 (1979).

[14] House hearings, *supra* note 12 (testimony of P. Walker, P. Quigley, P. Nugent, J. Stanton *et al.*)

[15] *See* Malley v. Briggs, —U.S.— (84-1586, Mar. 5, 1986), 54 U.S.L.W. 4243 (Mar. 5, 1986).

[16] 18 U.S.C. 2515.

[17] According to a recent poll, 77 percent of Americans are concerned about technology's threats to their personal privacy. Louis Harris & Associates, *The Road After 1984*, Southern New England Telephone (1984).

[18] *See* Dow Chemical v. United States, —— US. —— (May 19, 1984) (Powell, J. dissenting).

[19] For recent explorations on the capacity of Congress to interpret the Constitution, *see* Mikva, *How Well Does Congress Support and Defend the Constitution?*, 61 N.C. L. Rev. 587 (1983); Fisher, *Constitutional Interpretation by Members of Congress*, 63 N.C. L. Rev. 707 (1985).

[20] T. Harrington and B. Cooper, The Hidden Signals on Satellite TV (1984).

The equipment to complete an interception can be expensive, and the task difficult; however, the practice is sufficiently well known as to be an option for satellite dish owners and for foreign intelligence agencies. Despite the availability of the technical means of interception of microwave transmissions, such transmissions are protected by the plain language of Title III.

b. Cellular Telephone

In 1981 the Federal Communications Commission approved the use of cellular telephone services.[21] This technology uses both radio transmissions and wire to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wire.

In a cellular radiotelephone system, large service areas are divided into honeycomb-shaped segments or "cells"—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone, typically in a motor vehicle, moves from cell to cell.[22]

Cellular technology, because it is more complex, is more difficult to intercept than traditional mobile telephones; it is, however, more accessible than microwave transmissions. Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls.[23]

The availability of this technology poses a troubling conflict between the technology of surveillance and new techniques of communication using radio. Interception of cellular calls is illegal under current federal law.[24] At least one state has passed a law specifically aimed at protecting cellular calls.[25] Notwithstanding these legal proscriptions there remains a real-life conflict as interception technology catches up with communications development.[26] The resolution of these competing interests was carefully considered by the Committee.

---

[21] Cellular Communications Systems Decisions, 86 FCC 2d 469 (1981).

[22] House Hearings, *supra* note 12, testimony of P. Quigley, J. Stanton. Cellular technology is more advanced than ordinary mobile telephones. Cell-to-cell "hand-off" of calls maximizes channel capacity, allowing use by many more subscribers in a specific area. In addition, cellular telephone calls are fully automated and do not require the services of a mobile operator.

[23] *House Hearings, supra*, note 12 (testimony of R. Colgan), see Ad, Land Mobile Product News. Jan. 15, 1985 (for Regency scanners). When cellular service began it was "remarkably private". Huff, *Cellular Phone*, Technology Review, (Nov./Dec. 1983) at 53, 58. This was so because unlike older radio telephones there is usually no operator required to place the calls, and there is no party line function. Greathouse, *Privacy and the Cellular Phone*, Personal Communications Magazine. In addition, because cellular was assigned to new frequencies (between 825 Mhz and 890 Mhz), scanners were not initially available to easily enable scanning of cellular calls by the general public. *Id.* More recently, such scanners have been made available for sale. Hanson, *Legislating Cellular Privacy: An Idea That Won't Work*, Personal Communications Magazine; Corn, *The Privacy Issue*, Cellular Resources, 66, 71 (Sept/Oct 1984); Corn, *The Privacy Issue Updated*, Cellular Resources 46–49 (Nov. 1985).

[24] *See*, House Hearings, *supra* n. 12 (testimony of U.S. Dept. of Just.) (interception of cellular to landline calls illegal because "in whole or in part by wire." 18 U.S.C. 2510); *cf.* United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (same for ordinary mobile telephones); 47 U.S.C. 705 (interception and divulgence or use of communications not broadcast for general public illegal). Perhaps because of the relative newness of the technology, there are no cases directly addressing the issue of cellular interceptions.

[25] Cal. Penal Code §§630 *et seq.*

c. *Cordless Telephones*

Cordless telephones are another new telephone technology presenting a conflict between communication and interception. A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electrical current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios.[27]

The legality of intercepting cordless telephone calls has been fully litigated in only two states. The Supreme Courts of Kansas and Rhode Island, both construing federal law, have held that evidence obtained by an interception of a cordless telephone call by law enforcement officials without a warrant can be admitted at trial.[28] In each case the court was convinced that the radio portion of a conversation was entitled to no legal protection against interception.[29] This approach sharply conflicts with the major relevant federal case.[30]

These courts were not required, however, to decide the rights of the other party to the conversations in these cases, persons using conventional landline telephones. While it it possible to argue that a person using a cordless phone knows or has reason to know that the call can be easily overheard, that argument does not apply to the other party to the conversation.

DATA TRANSMISSIONS AND ELECTRONIC MAIL

When Congress enacted the Wiretap Act it specifically excluded the transmission of data from protection against private and governmental interceptions.[31] In the intervening years, data transmission and computer systems have become a pervasive part of the business and home environments.

Computer and telephone technologies have merged; the resulting new communication techniques utilize computer terminals and video display screens, and frequently transmit data over telephone lines.

---

[26] House Hearings, *supra* note 12 (testimony of R. Colgan). The wide availability of this technology and its expanded use of up to 7 million such phones by 1990, poses additional challenges to law makers.

[27] *See* State v. DeLaurier, 488 A.2d 688 (R.I. 1985); State v. Howard, 235 Kan. 236, 679 P.2d 297 (1984).

[28] 488 A.2d 688; 235 Kan. 236, 679 P.2d 297.

[29] 488 A.2d 688; 235 Kan. 236, 679 P.2d 297. The state courts concluded that radio communications are neither "wire" nor protected "oral communications". 488 A.2d at 693; 235 Kan. at 247 They reasoned that to require the police to obtain a warrant to listen to an AM radio would be "absurd". 488 A.2d at 694. They also reasoned that such communications were not protected against interception because there is no "reasonable expectation of privacy". State v. DeLaurier, 488 A.2d at 694. State v. Howard, 235 Kan. 236, 676 P.2d 297 (1984). The *DeLaurier* court also found that an AM radio is not a "device" within the meaning of 18 U.S.C. 2510(5), therefore no violation of federal law occurred. 488 A.2d at 694.

[30] United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (interception of radio portion of mobile telephone call violates Wiretap Act since communication "in whole or in part by wire." 18 U.S.C. 2510.

[31] 1968 Senate Report, *supra* note 7, at 90.

The array of services include electronic bulletin boards, electronic data bases, videotext services, and remote computing. Some of these new services permit an individual to use a keyboard and telephone to transmit electronic messages and data and to receive interactive services featuring banking and other financial services, shopping, news, messages, and education. Many of these services also record the nature of the transactions engaged in by the user. Thus, the new technologies represent both an explosion in communication opportunities as well as surveillance possibilities.[32]

One of the most popular new computer services is electronic mail, a service which combines features of the telephone and regular first class mail. Electronic mail can include telex, teletex, facsimile, voice mail and mixed systems that electronically transmit and store messages. Many e-mail users have found it a useful substitute for telephone calls, while others utilize it instead of the government postal service.

Electronic mail differs from regular mail in three ways. First, e-mail is provided by private parties and thus not subject to governmental control or regulation under the postal laws.[33] Second, it is interactive in nature and can involve virtually instantaneous "conversations" more like a telephone call than mail. Finally, e-mail is different from regular mail because the electronic communication provider as part of the service may technically have access to the contents of the message and may retain copies of transmissions.[34]

Any discussion of the application of current law governing interception of e-mail or the use of e-mail surveillance begins with the Fourth Amendment, which protects our reasonable expectation of privacy. There are no reported cases governing the acquisition of e-mail by the government, so an application of the Fourth Amendment to the interception of e-mail is speculative. It appears likely, however, that the courts would find that the parties to an e-mail transmission have a "reasonable expectation of privacy" and that a warrant of some kind is required.

As for statutory protection, while there may be some limits on government access to e-mail messages from an e-mail provider, there do not appear to be any federal statutes which directly address this issue.[35] Title III would not apply, since it is limited to the "aural acquisition" of the contents of a communication, and e-mail usually does not involve the transmission of audible sound.[36] The Communications Act might have some limited application, excepting law enforcement officials.[37] The Foreign Intelligence Sur-

---

[32] OTA Report, *supra* note 9, at 48.

[33] *See* 18 U.S.C. 1701 *et seq*. These regulations appear to place restrictions on government access to government operated electronic mail systems. Although the United States Postal Service operated an electronic mail system for a short period, that service is no longer in operation.

[34] House Hearings, *supra* note 11 (testimony of P. Walker). E-mail systems are designed to provide access to contents and copies of messages in case of system failure. Messages are electronically generated and not normally accessed by the e-mail provider.

[35] The Right to Financial Privacy Act may apply if certain categories of records are involved. 12 U.S.C. 3401 *et seq*.

[36] *See* 18 U.S.C. 2510; United States v. New York Telephone Company, 434 U.S. 159, 168 (1977).

[37] 47 U.S.C. 705 (which bars the interception and disclosure or use of certain communications) applies only to radio or wire communications. Some courts have held that this statute does not

Continued

veillance Act, however, could be read to require federal law enforcement officials to obtain a court order before engaging in "electronic surveillance" that acquires the contents of e-mail communications.[38] These criminal prohibitions do not apply to private persons.

REMOTE COMPUTING SERVICES

The use of remote computing services has also dramatically increased.[39] Many persons use the facilities of these services to process and store their own data.

A subscriber or customer to a remote computing service transmits records to a third party, a service provider, for the purpose of computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.

As with electronic mail, remote computing services are still relatively new, and there is no case law directly on point. Proceeding by analogy, under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services.[40] It is likely, however, that contents of customer data enjoy a higher degree of Fourth Amendment protection.[41]

PAGING DEVICES

An increasingly important adjunct to the telecommunications systems is the paging system. Radio paging is essentially a one-way message service. Recent estimates indicate that there are over 2.5 million pagers in operation; these numbers are expected to double within five years.[42]

There are three basic types of paging devices: tone-only, digital, and voice.[43] In a tone-only pager system an outside party places a telephone call to the paging service which in turn sends a signal to the user indicating that the user has a telephone call. The user must then call back a specific phone number (often an answering service). The digital or display pager permits the user to receive a

---

govern the activities of law enforcement officials. United States v. Hall, 488 F.2d 193, 197 (9th Cir. 1973); United States v. Chrisman, 375 F. Supp. 1354 (N.D. Cal. 1974).

[38] 50 U.S.C. 1809(a) provides that it is a felony for a person to "engage in electronic surveillance under color of law except as authorized by statute." 50 U.S.C. 1801(f) includes within the definition of "electronic surveillance" "the acquisition . . . of the contents of any wire or radio communication . . ." 50 U.S.C. 1801(f).

[39] House Hearings, *supra* note 12 (testimony of P. Nugent).

[40] Cf. United States v. Miller, 425 U.S. 435 (1976) (no standing under Fourth Amendment for customer to object to bank disclosure of customer records). Congress reversed the result reached in *Miller* by enacting the Right to Financial Privacy Act, 12 U.S.C. 3401 et. seq.

[41] *Miller*, note 39 *supra*, might be distinguished when contents rather than records are involved. Unlike records of the bank's (or remote computing service's) records, contents are analogous to items stored, under the customer's control, in a safety deposit box.

[42] According to one consultant for Authur D. Little, the number of pagers in service could grow to 10 million (including 6 million display pagers) by 1990. *Telocator Members Told That Paging to Prosper in the Future*, TELOCATOR BULLETIN, September, 1984.

[43] *See generally*, Note, *Does A Part Equal the Whole: Is the Interception of Paging Devices Communications Governed by Title III*, 7 GEO. MASON U.L. REV. 234 (1984). Newer two-way paging devices are apparently on the horizon. Posa, *Radio Pagers Expand Horizons*, HIGH TECHNOLOGY (March, 1983).

digital or alphanumeric message on a display screen. A voice pager permits a person who wishes to communicate with the user to leave a recorded message which is then transmitted to the user. The user actually hears the voice message.

The only reported case on this technology, *Dorsey* v. *State,*[44] involves a voice pager. In the *Dorsey* case, the court upheld the use of a scanner by the police to intercept voice messages transmitted over a paging system to an alleged drug dealer. The court held that these messages are neither wire nor oral communications and, therefore, such interceptions are lawful.[45]

According to the United States Department of Justice, however, the three types of paging devices require different levels of statutory protection.[46] The Department reasons that "tone only" pagers carry no reasonable expectation of privacy and therefore no court order is required for a government official to intercept or monitor such signals. The interception of "display pagers" is, according to the Department of Justice, also not within the ambit of Title III; the Department concedes, however, that because, use of such devices encompasses a reasonable expectation of privacy, governmental interception of messages over such a system requires use of a search warrant under the Fourth Amendment.[47] Finally, the Department of Justice concludes that a "voice pager" is simply the continuation of an original wire communication, and therefore a Title III court order is required.[48]

PEN REGISTERS

The privacy of telephone customers can also be affected by the use of pen registers or other devices which record the numbers dialed from a telephone.[49] Pen registers can be used by telephone companies for internal business purposes[50] as well as by the government for law enforcement purposes.[51] It is this governmental use which has posed the most difficult questions for Congress and the courts.[52]

---

[44] 402 So. 2d 1178 (Fla. 1981). In *Dorsey*, the Supreme Court of Florida interpreted a state statute *in para lateria* with Federal law. 402 So. 2d at 1183.

[45] *Id.* The *Dorsey* court specifically rejected the reasoning in United States v. Hall, 488 F.2d 193 (9th Cir. 1973).

[46] U.S. Department of Justice, Office of Legal Counsel (Theodore B. Olson), Memorandum for John A. Mintz, Assistant Director-Legal Counsel, Federal Bureau of Investigation, January 5, 1984 (Olson Memo).

[47] Olson Memo, *Supra* note 40.

[48] *Id. Compare,* Dorsey v. State, 402 So. 2d 1178 (Fla. 1981).

[49] *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 161, 167 (1977); United States v. Giordano, 416 U.S. 505, 549 n. 1 (1974) (Powell, J., concurring in part and dissenting in part).

[50] Telephone companies can use pen registers to verify long distance billing information. Fishman, *Pen Registers and Privacy: Risks, Expectations and the Nullification of Congressional Intent,* 29 Catholic L. Rev. 557, 558 (1980). Telephone companies can use pen registers to detect the use of illegal devices, such as "blue boxes." United States v. N.Y. Tel. Co. 434 U.S. 159, 174-75 (1977); *See generally* Note, *The Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool,* 60 Cornell L. Rev. 1028, 1029 (1975). Additionally, a pen register could be placed on the phone of a person suspected of placing harrassing or obscene calls. 47 U.S.C. 223. *See generally* Claerout, *The Pen Register,* 20 Drake L. Rev. 108, 109-110 (1970).

[51] Pen registers are often used to acquire "probable cause" evidence necessary to obtain a search warrant or a Title III wiretap order. House Hearings, *supra* note 12 (testimony of J. Knapp). Remarks, Fred Hess, Criminal Division, United States Department of Justice, Office of Technology Assessment Workshop, May 17, 1985. *See also* Fishman, Wiretapping and Eavesdropping 46 (1978).

[52] Slightly different issues are presented when law enforcement officials utilize devices which trap or trace incoming phone calls. Prior to the passage of Title III courts had upheld the use of

Continued

The United States Supreme Court has on two occasions decided cases involving questions about the legality of installation and use of pen registers. *United States* v. *N.Y. Tel. Co.*[53] presented the question whether an ordinary search warrant was sufficient to authorize government use of a pen register. The Court held that the existing federal wiretap law was not implicated by the use of a pen register,[54] and that federal district judges have authority to issue warrants directing telephone company cooperation with the installation of pen registers.[55]

In *Smith* v. *Maryland*[56] the Supreme Court found that law enforcement officials need not obtain a search warrant before securing telephone company cooperation in the installation of a pen register.[57] The Court reasoned that because the person who used the telephone voluntarily disclosed the numbers dialed there was "no reasonable expectation of privacy," eliminating Fourth Amendment protection.[58]

The current practice of federal law enforcement agencies is to obtain a court order, under Rule 57 of the Federal Rules of Criminal Procedures,[59] before using a pen register.[60] This practice conforms with the Foreign Intelligence Surveillance Act,[61] which created a requirement for a court order even in a domestic criminal case.[62] Outside the limited context of foreign intelligence, Congress has specified no standard for obtaining a pen register court order. Thus, current case law and statutes leave federal law enforcement officials with virtually unchecked discretion to obtain information through the use of pen registers. All the government needs to do is make an application to a federal court; no independent judicial review of the facts is required.

RECORDS

Electronic communication technologies have become so pervasive that extensive records are maintained which reveal a great deal about how individuals interact with each other. For decades, telephone companies have maintained telephone toll records and tele-

---

such devices because of the consent of one of the parties to the communication. Rathun v. United States, 355 U.S. 107 (1957). Enactment of Title III has not affected this result. Carr, THE LAW OF ELECTRONIC SURVEILLANCE, § 3.03[3] at 84 (1977) and at 23 (1985 Supp.).

[53] 434 U.S. 159 (1977).

[54] *Id. at* 165–68.

[55] *Id. at* 171–78.

[56] 442 U.S. 735 (1979).

[57] *Id.* at 746.

[58] *Id.* at 745.

[59] The Rule specifies: In all cases not provided for by rule, the district judges and magistrates may regulate their practice in any manner not inconsistent with these rules or those of the district in which they act. FED. R. CRIM. PROC. 57.

[60] The Subcommittee on Courts, Civil Liberties and the Administration of Justice of the Committee on the Judiciary, United States House of Representatives, conducted a survey of all 94 federal district court Chief Judges to ascertain how frequently pen registers are used. The Subcommittee received 60 responses which indicated that for those courts 2,199 pen register orders were obtained during the first 9 months of 1985.

[61] Public Law 95–511; 50 U.S.C. 1801 *et seq.*

[62] 50 U.S.C. 1809 creates criminal liability for federal officials who engage in electronic surveillance, unless such official has either a search warrent or a court order from a court of competent jurisdiction. 50 U.S.C. 1801(f) defines "electronic surveillance" to include the acquisition of the "contents" of wire communications, and further defines "contents" to "include any information concerning the identity of the parties to such communication or the existence, substance, purpont or meaning of that communication." Thus, the Foreign Intelligence Surveillance Act covers the use of pen registers. H.R. Rep. No. 1293; 95th Cong. 2d Sess. 67 (1978).

graph companies have kept copies of telegrams. There is a body of law which addresses the question of government access to this data.[63] Similarly there are legal rules which limit the access to information about postal correspondence.[64]

The newer technologies such as electronic mail and remote computing services maintain a type of records which do not neatly fit within the legal categories which exist for older technologies. This legal uncertainty has caused concern within the business community for several reasons. First, to the extent that potential customers have less protection when they use an electronic medium than with paper, there may be a disincentive to use an electronic service.[65] Second, if persons with records have a choice of maintaining them "in house" or with a third party, they may be less inclined to go outside if such a move deprives them of legal rights (such as notice and an opportunity to contest government access). Any effort to resolve this legal uncertainty should first proceed from a complete understanding of the existing law with respect to more traditional technologies.

Telephone toll records

As a general matter telephone companies maintain a record of calls placed from a telephone for billing purposes. These business records are primarily used by the telephone company for its own purposes. At the federal level the government can legally obtain access to such records based on a grand jury or trial subpoena or through the use of an administrative summons authorizing a specific federal agency to obtain records.[66] Such government access is usually in connection with an ongoing criminal or civil investigation.[67] The most frequent use of this investigative technique is by the Department of Justice.[68] Requests for telephone toll records would appear to easily exceed 100,000 per year.[69]

At the state level, some states have placed limits on access to telephone toll records by state and local law enforcement. Colorado,[70] California,[71] Pennsylvania,[72] and New Jersey,[73] have all required that a court order be obtained before access to telephone-created transactional information can be granted. The majority view, however, appears to conform with federal law, that is to permit access based on any form of legal process.[74]

---

[63] *See generally.* Reporters Committee v. AT&T 593 F.2d 1030 (D.C. Cir. 1979) *cert. denied*, 440 N.S. 949 (1979) (no violation of the Fourth Amendment to release toll call records without notice to the customer); *see also* Smith v. Maryland, 442 U.S. 735 (1979) (use of a "pen register is permissible under Fourth Amendment because a subscriber has no reasonable expectation of privacy in numbers dialed.)

[64] 39 U.S.C. 3263(d) (requires search warrant to open first class mail); United States v. Van Leeuwen, 397 U.S. 249 (1970) (first class mail may only be opened pursuant to warrant under Fourth Amendment); Ex parte Jackson, 96 U.S. 727, 733 (1878) ("whilst in the mail . . . [letters] . . . can only be opened and examined under . . . warrant").

The use of mail covers, which record the names and addresses of senders and recipients of mail, have different legal standards applied to their use. Because investigative use of this information does *not* include access to the contents of the lettes there has been a lesser degree of Fourth Amendment concern. *See* note 2, *infra*.

[65] *See* House Hearings, *supra* note 12, testimony of M. Nugent.

[66] Reporters Comm. v. AT&T, *supra* note 61.

[67] *Id.*

[68] *Id.*

[69] The Committee conducted a survey of various telephone companies to ascertain the frequency with which telephone toll records are sought. For approximately six states (Maryland, Washington, D.C., Colorado, Michigan, Illinois and most of California) nearly 10,000 subpoenas were issued by the Department of Justice for a one year time period. NYNEX reported that for New York State alone, subpoenas were received *relating to* between 35,000 and 91,000 telephones per year over the past five years.

In Reporters Comm. v. AT&T, *supra*, note 61, at 1037, it was estimated that the number of requests for telephone toll records was at a rate of between two and three thousand each month.

Telegrams

The applicable federal law would appear to permit governmental access to copies of telegrams based on the use of a subpoena.[75]

First class mail searches and mail covers

One of the most frequently used forms of private communication is the government operated first class mail system. Therefore, an assessment of the limitations which have been placed on governmental access to the contents of and/or transactional information concerning first class mail correspondence is relevant to any determination about what legal rights should exist with respect to access by the government to newer forms of communications.

Under current Federal law, a search warrant based on probable cause is required before the government can obtain the contents of a first class letter.[76]

A lower standard is used for government access to mail covers, an investigative technique whereby the postal service records the names and addresses of persons who write to an investigative target or to whom such person writes. While the United States Postal Service does place limits (by regulation) on the use of this technique, courts have thus far declined to find a Fourth Amendment interest implicated by the practice.[77]

STATEMENT

Legislation amending the Wiretap Act to include new technologies, H.R. 214, was first introduced in the 95th Congress by Congressman Robert W. Kastenmeier, Chairman of the Subcommittee on Courts, Civil Liberties and the Administration of Justice of the

---

[70] People v. Sporleder, 666 p.2d 135 (Sup. Ct. Colo. 1983), Charnes v. diGiacomo, 612 F2d 1717 (Sup. Ct. Colo. 1980), People v. Corr, 682 P.2d 20 (Sup. Ct. Colo. 1984).

[71] People v. Blair, 25 Cal. 3d 640, 602 P.2d 738 (Calif. Sup. Ct. 1979); People v. McKunes, 124 Cal. Rep. 126 (Calif. Ct. App. 1975).

[72] Commonwealth v. DeJohn, 986 Pa. 32, 403 A.2d 1283 (1979), *Cert. denied*, 444 U.S. 704 (1980).

[73] State v. Hunt, 91 N.J. 338, 450 A.2d 952 (1982); Note, 13 Seton Hall L. Rev. 803 (1983).

[74] In re Order for Indiana Bell Telephone to Disclose Records 409 N.E. 2d 1089 (Sup. Ct. Ind. 1980); State v. Fredette, 411 A.2d 65 (Sup. Ct. Me. 1979); Hastetter v. Behan, 639 p.2d 10 (Sup. Ct. Montana. 1982); People v. DiRaffaele, 55 N.Y. 2d. 234, 433 N.E. 513 (Ct App. 1981); Fitzgerald v. State, 599 p.2d 572, 577 (Sup. Ct. Wyo. 1979).

[75] Wheeler v. United States, 226 U.S. 478 (1913) (a subpoena requiring production of telegrams upheld against a Fourth Amendment challenge); *see also* Brown v. United States, 276 U.S. 134 (1928) (upholding finding of criminal contempt against person who refused to comply with subpoena of copies of telegrams).

[76] *See* note 62, *supra.*

[77] 39 C.F.R. 233.2; United States v. Krauth, 769 F.2d 473 (8th Cir. 1985) United States v. Gering, 716 F.2d 615 (9th Cir. 1983); United States v. Depoli, 628 F.2d 779 (1980); United States v. Huie, 593 F.2d 14 (5th Cir. 1979); United States v. Choate, 576 F.2d 165 (1978); and 619 F.2d 11 (9th Cir. 1980); Vreeden v. David, 718 F.2d 343 (10th Cir. 1983); *see also* Paton v. LaPrade, 469 F.Supp. 773 (D.N.J. 1978). See generally Burnham, *Keeping an Eye on Suspect Mail, New York Times*, March 1, 1986, pg. B-10.

House Committee on the Judiciary. That legislation grew out of widespread general concern with government surveillance.[78]

Although H.R. 214 was not enacted, Congressman Kastenmeier revisited the subject in general oversight hearings held in the 98th Congress entitled "1984: Civil Liberties and the National Security State." [79]

As a result of those hearings, a bill, H.R. 6343, was introduced in the 98th Congress by Congressman Kastenmeier that served as a model for legislation in the 99th Congress.

During the 99th Congress, the Committee, acting through the subcommittee on Courts, Civil Liberties, and the Administration of Justice—held four days of hearings on H.R. 3378 the bill on which H.R. 4952 is based, introduced by Chairman Kastenmeier and Cong. Carlos J. Moorhead, ranking minority Member of the Subcommittee. An identical bill, S. 1667, was introduced in the Senate by Sen. Patrick J. Leahy, ranking minority Member of the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary, and Sen. Charles McC. Mathias, Chairman of the Subcommittee .

On September 26, 1985, the Subcommittee heard from the following witnesses: Senator Patrick Leahy (United States Senator from Vermont); Philip M. Walker (general regulatory counsel, GTE Telenet Inc., on behalf of the Electronic Mail Association); and Philip J. Quigley (president and chief executive officer, Pactel Mobile Companies, on behalf of the Cellular Telecommunications Industry Association).

On October 24, 1985, the subcommittee heard from Fred W. Weingarten (program manager, communication and technologies program, Office of Technology Assessment, United States Congress); P. Michael Nugent (government affairs counsel, Electronic Data Systems Corporation, on behalf of ADAPSO, the computer software and services industry association); and John Stanton (executive vice president, McCaw Communications Companies, Inc., on behalf of Telocator Network of America).

On January 30, 1986, the subcommittee took testimony from Neal Amick (division manager for corporate security, American Telephone and Telegraph Company); John W. Kelly Jr. (attorney, Southwestern Bell Telephone Company); Perry Williams (secretary, American Radio Relay League, Inc., a group representing ham radio operators, presenting the statement of Dr. Larry E. Price, president of the group); George A. Kuhnreich, (vice president for corporate planning and governmental affairs, Tandy Corporation); and Richard T. Colgan (executive secretary, Association of North American Radio Clubs).

On March 5, 1986, the final day of hearings, the witnesses were James I. K. Knapp (Deputy Assistant Attorney General, Criminal Division, United States Department of Justice); and Clifford F. Fishman (Professor of Law, Columbus School of Law, Catholic University of America, and author of *Wiretapping and Eavesdropping.*

---

[78] *See generally Surveillance: Hearings on the Matter of Wiretapping, Electronic Eavesdropping, and Other Surveillance Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice of the House Comm. on the Judiciary*, 94th Cong., 1st Sess.

[79] *1984: Civil Liberties and the National Security State: Hearings Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice*, 98th Cong., 1st and 2d Sess. 133–258.

The Subcommittee took note that the Senate held a hearing on S. 1667, on November 13, 1985.

After completion of the hearing process in the 99th Congress, H.R. 3378, the bill on which H.R. 4952 is based, went to subcommittee mark-up on May 14, 1986. Two amendments, offered by Mr. DeWine, were not accepted by the subcommittee. A quorum of Members being present, the bill, as amended by Chairman Kastenmeier by an amendment in the nature of a substitute, was passed by a voice vote and reported in the form of a clean bill. H.R. 4952 was introduced by Mr. Kastenmeier on June 5, 1986, cosponsored by 14 Members of the subcommittee and 10 other Members: Mr. Moorhead, Mr. Brooks, Mr. Mazzoli, Mr. Synar, Mrs. Schroeder, Mr. Frank, Mr. Morrison of Connecticut, Mr. Berman, Mr. Bouncher, Mr. Hyde, Mr. Kindness, Mr. Swindall, Mr. Coble, Mr. Edwards of California, Mr. Conyers, Mr. English, Mr. Matsui, Mr. Bruce, Mr. Owens, Mr. Mitchell, Mr. Kostmayer, Mr. Nowak, and Mr. Leland.

On June 10, 1986, the full Committee considered H.R. 4952 and, after general debate, and without substantive amendment, ordered the bill reported favorably by roll call vote, 34-0, a quorum of Members being present.

SUPPORT FOR THE LEGISLATION

The organizations and individual corporations named below support the principles embodied in the legislation.

Organizations

Electronic Mail Association
ADAPSO (Computer software and services industry association)
Telocator Network of America
Cellular Telecommunications Industry Association (CTIA)
American Civil Liberties Union (ACLU)
National Association of Manufacturers (NAM)
U.S. Chamber of Commerce
National Association of Broadcasters (NAB)
National Cable Television Association (NCTA)
National Association of Business & Educational Radio (NABER)
American Radio Relay League (ham operators)
CBEMA (Computer and Business Equipment Manufacturers Association)
U.S. Telephone Association
Videotext Industry Association
Information Industry Association
Electronic Funds Transfer Association
Radio and Television News Directors Association
Association of American Railroads
Institute of Electrical and Electronics Engineers (IEEE)
Direct Marketing Association
Utilities Telecommunications Council
Associated Credit Bureaus, Inc.

Corporations

AT&T
General Electric
IBM
GTE
ITT
MCI
CBS
Capital Cities/ABC, Inc.
National Broadcasting Co., Inc. (NBC)
Tandy Corporation (Radio Shack)
EDS, a subsidiary of General Motors Trintex
Equifax
TRW
Source Telecomputing Corporation
Chase Manhattan Bank
Motorola
Ameritech
Bell Atlantic
Bell South
Southwestern Bell
NYNEX
Pacific Telesis
US West
Associated Credit Services, Inc.

AGENCY VIEWS

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AND INTERGOVERNMENTAL AFFAIRS,
Washington, DC, June 6, 1986.

Hon. PETER RODINO, Jr.,
Chairman, Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: This letter is to advise you of the Department of Justice's position with regard to H.R. 4952, the Electronic Communications Privacy Act of 1986, which we understand is scheduled for markup on June 10 by the full House Judiciary Committee. This bill makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the members and staff of the Subcommittee on Courts, Civil Liberties and the Administration of Justice, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of H.R. 4952.

Sincerely,

JOHN R. BOLTON,
Assistant Attorney General.

SECTION-BY-SECTION ANALYSIS

Section 1 provides the short title for the bill, the Electronic Communications Privacy Act of 1986.

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

Section 101 contains five subsections. Subsection (a) contains the definitions, and amendments to definitions, used in this chapter and in the new chapter 121 of title 18.

Subsection (a)(1) contains three subparagraphs. Subsection (a)(1)(A) amends the definition of "wire communication" to include aural transfers. The term "aural transfer" is defined in section 2510 (18) of this title. The term "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and point of interception. Thus, the amended definition is intended to encompass existing telephone services.[80] Digitized voice communications are included to the extent that the communication originates with human voice. As a result of this change, a company whose activities affect interstate commerce and which installs its own private telephone or electronic communication system would have that system covered by the statute.

By amending the definition of "wire communication" in subsection (a)(1)(8) to include communications utilizing wires, cables, or other like connections within a switching office, the Committee intends that "wire communication" be construed to include communications made over cellular systems (as defined in 47 C.F.R. § 22.2),[81] regardless of whether the communications are between two cellular telephones or between a cellular telephone and a "landline" telephone.

Existing law, which prohibits interception of wire communications or oral communications, was enacted prior to the development of cellular telecommunications and does not provide adequate privacy protection to conversations transmitted over a cellular system. The Department of Justice has taken the position that, under existing law, communications between a mobile radio telephone and a landline telephone are wire communications, but that conversations between two radio telephones and not carried in whole or in part by regular telephone lines are neither wire communications nor oral communications. Inasmuch as all cellular communications (whether mobile-to-mobile or mobile-to-landline) must pass through a mobile telephone switching office, the Committee bill will remedy this inadequacy and provide explicit privacy protection to all communications utilizing cellular radio.

---

[80] The term "other like connection" as used in section 2510(1) includes fiber optic cable.

[81] *Cellular System.* A high capacity land mobile system in which assigned spectrum is divided into discrete channels which are assigned in groups to geographic cells covering a geographic service area. The discrete channels are capable of being reused in different cells within the service area.

In the event that the evolution of cellular technology permits the switching or transmission of mobile-to-mobile service (or mobile-to-landline service) without the use of wire, cable, or other like connection, the Committee intends that cellular communications be included within the term "electronic communication". Because cellular communication is transmitted over a communication system currently regarded by the FCC as a common carrier,[82] the Committee also intends that such communication not be considered "readily accessible to the general public" at any time subsequent to the date of enactment, regardless of how a provider of cellular service is denominated by any state or how the FCC may classify any such provider in the future.

The Committee's intention of providing privacy protection to cellular communications in any event is also reflected in the specific inclusion in the legislation of penalties for the interception of such communications.[83]

Part of the impetus to clarify the illegality of interception of cellular communications has been provided by the advertisement of scanning receivers (popularly known as "scanners") specifically promoting eavesdropping on conversations transmitted over cellular systems. Apparently after the FCC allocated frequencies to cellular radio some manufacturers of scanners added the capability to stop at and receive signals transmitted on these frequencies. The Committee finds this development troubling, and expects that the future design and manufacture of scanners will take into account the privacy protections accorded cellular telephony in this legislation.

Section 101(a)(1) amends the definition of "wire communication" to include "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection * * * furnished or operated by any person engaged in providing or operating such facilities for the transmission of * * * *communications affecting interstate or foreign commerce* * * *." Similarly, section 101(a)(5) defines a new term "electronic communication" to include "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a * * * *system that affects interstate or foreign commerce* * * *."

By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example, it, like the Omnibus Crime Control and Safe Streets Act of 1968, regulates only those "interceptions" conducted within the territorial United States. *See Stowe* v. *Devoy*, 588 F.2d 336 (2d Cir. 1978), *cert. denied*, 442 U.S. 931 (1979), and cases cited therein. *See also Berlin Democratic Club* v. *Rumsfield*, 410 F.Supp. 144, 157 (D.D.C. 1976), *United States* v. *Toscanino*, 500 F.2d 267, 279–280 (2d Cir. 1974); *Unites States* v. *Cotroni*, 527 F.2d 708 (2d Cir. 1975). Similarly, the controls in section 201 of the Act regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States.

---

[82] *See* Cellular Communications Systems, 86 FCC 2d 469, 496 (1981).

[83] *See* 18 U.S.C. § 2511(4)(b), *as added by* § 101(d)(2) of H.R. 4952.

Subsection (a)(1)(C) amends the definition of wire communication to delete the "common carrier" requirement. In the current environment, numerous entities provide electronic communications services beyond the traditional common carrier. Therefore, the Committee chose to extend federal jurisdiction to the maximum permissible constitutional limits by providing coverage of a person who provides or operates facilities for communications that affect interstate or foreign commerce. *See Heart of Atlanta Motel* v. *United States, 379 U.S. 241, 258-259 (1964).*

In the present telecommunications environment, a terminating or originating customer or subscriber will often have installed his own facilities to switch or otherwise process his incoming or outgoing traffic. One example of such equipment is the "private branch exchange", or PBX, typically owned or leased by the customer and located on his premises, and used to interconnect the customer's telephones and date terminals with one another and with the lines of the local exchange carrier, one or more interexchange carriers, and possibly other service providers. To the extent that electronic and wire communications passing through PBXs and other such equipment affect interstate commerce, the Committee intends that those communications tbe protected under Section 2511. The interception of an electronic or wire communication at a point on the customer's premises is thus as much a violation of Section 2511 as if the interception were made through the equipment of a communications carrier. Similarly, where a user has interconnected its own equipment into a private network, communications carried on the network are fully entitled to the protections of Section 2511.

Subsection (a)(1)(D) amends the definition of wire communication to exclude the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

By "cordless telephone" we refer *not* to a cellular telephone, but to the type of telephone which uses a short range (a few hundred feet) radio link between the handset and the base unit in place of the usual wire. Such telephones are regulated under Part 15, subpart E of the rules of the Federal Communications Commission (FCC), and are not licensed. Because the communications made on some cordless telephones can easily be intercepted with readily available technologies (such as AM radio), it would be inappropriate to make such interception a criminal offense. The absence of privacy protection has been noted by the FCC. 47 C.F.R. § 15.236(a) (requiring a label stating "PRIVACY OF COMMUNICATIONS MAY NOT BE ENSURED WHEN USING THIS PHONE"). This view also comports with some recent cases. *See* discussion of current law, *supra*. It should be noted that it is only the *radio portion* of the communication that is excluded. The wire portion of the communication remains fully covered in the same sense as a traditional wire telephone conversation.

Subsection (a)(2) amends the definition of oral communication to exclude electronic communications. An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, rather than by an electronic medium.

The definitions of wire communication and oral communication are not mutually exclusive. Accordingly, different aspects of the same communication might be differently characterized. For example, a person who overhears one end of a telephone conversation by listening in on the oral utterances of one of the parties is intercepting an oral communication. If the eavesdropper instead taps into the telephone wire, he is intercepting a wire communication. There have been cases involving radio communications in which the court having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The Committee views this as an inappropriate consideration and the amendment to 18 U.S.C. 2510(2) rejects that case analysis. *See, e.g., United States v. Rose,* 669 F.2d 23 (1st Cir. 1982).

Subsection (a)(3) amends section 2510(4) of title 18 to provide a definition for the term "intercept" with respect to electronic communications. The definition under current law of "intercept" is retained with respect to "wire" and "oral communications" with one exception. The Committee added the term "or other" after "aural". This change is intended to make clear that it is illegal to intercept the non-voice portion of a wire communication such as the data or digitized portion of a voice communication. The term intercept with respect to "electronic communications" is defined to mean "the interception of the contents of that communication through the use of any electronic, mechanical or other device".

Subsection (a)(4) amends section 2510(3) to strike the words "identity of the parties to such communication or the existence". This amendment avoids any ambiguity about the legality of the use of "pen registers". The Supreme Court has clearly indicated that the use of pen registers does not violate either this chapter or the Fourth Amendment. This amendment makes that policy clear. In addition, this amendment should be read in conjunction with the new chapter on pen registers, chapter 206 of title 18. It does not, however, affect the installation on use of pen registers under the Foreign Intelligence Surveillance Act. 50 U.S.C. 1801 *et. seq.* This amendment also makes clear the distinction between contents of communications and transactional records. The omission of a conforming amendment to the definition of "contents" in section 705 of title 47 is not intended to affect the current law under that section with respect to pen registers. The use of pen registers has been found not to violate section 705. *See Hodge* v. *Mountains Tel. & Telegraph Co.,* 555 F.2d 254 (19th Cir. 1977).

Subsection (a)(5) adds six new definitions to the chapter. Section 2510 is amended by adding a new subsection (12) to define "electronic communications". This expansion permits the inclusion in the general wiretapping and bugging law of many new forms of communication. For example, digitized transmissions and electronic mail will be provided with protection against interception. The definition of electronic communication means "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include any wire or oral communication." Excluded from the definition of "electronic communication" are: (1) the radio portion of a cordless telephone communication; (2) any wire or oral communication; (3) any communication by a tone-only paging device; or (4) any communication from a tracking device.

The term "electronic communication" is intended to cover a broad range of communication activities that affect interstate or foreign commerce, except that the term does not include either oral or wire communications. As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire). Communications consisting solely of data, for example, and all communications transmitted only by radio would be electronic communications.

A wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fibre-optic cable or by radio—as in the case of cellular telephones and long-distance satellite or microwave facilities. This result is generally in accord with the case law. *See United States* v. *Clegg*, 509 F.2d 605, 611 (5th Cir. 1975); *United States* v. *Gregg*, 629 F. Supp. 958, 963 (W.D. Mo. 1986). Moreover, the conversion of a voice signal to digital form for purposes of transmission does not, in itself, render the communication non-wire; the provider's choice of transmission technology should not be dispositive. The Committee has intentionally omitted from the definitions any indication that a wire communication cannot also exhibit some of the characteristics of an electronic communication.

It should be noted that an improperly mechanical reading of the phrase "in whole or in part * * * by the aid of wire * * *" could sweep in virtually all voice communications made with the aid of any electronic equipment, inasmuch as virtually all such equipment includes in its assembly some length of wire or the equivalent. The Committee, however, intends the quoted phrase to refer to wire that carries the communication to a significant extent from the point of origin to the point of receipt, and not to wire that is found inside the terminal equipment at either end of the communication. On the other hand, communications over a length of wire that connects two telephones in the same building would be protected as wire communications. Similarly a cellular telephone system which uses either the wire-line system or wires in a switching station is covered as a wire communication.

A transaction may consist, in parts, of both electronic communications and wire or oral communications. For example, the transmission of data over the telephone is an electronic communication; but if the parties used the line to speak with one another between data transmissions, they would then be making a wire communication. And, indeed, a party's utterances into the telephone mouthpiece are an oral communication. The rules governing interception or disclosure may be different for each type of communication. The Committee understands that the Department of Justice will apply for a court order under the "wire" standards in cases where a tap may intercept mixed wire and electronic communications. As long as the wire standards are followed a single court order should suffice to authorize the interception of both wire and electronic communications involving the same lines or instruments.

Inclusion of the term "radio" in the definition of "electronic communication" in Section 2510(12) reflects the fact that radio communications come within the scope of chapter 119. A number of other provisions, however, affect the legality of the interception of radio communications under chapter 119. The Committee does not intend any of the provisions directed specifically to radio to affect the applicability of Section 705 of the Communications Act of 1934, as amended, to actions by members of the public.

Subsection (a)(5) also adds a definition for the term "user." "User" means any person or entity who uses an electronic communication service and is duly authorized by the provider of such service to engage in such use.

Interception of closed circuit television communications is only included in the bill in a limited fashion. If a person or entity transmits a closed circuit television picture of a meeting using wires, microwaves or other method of transmission, the transmission itself would be an electronic communication and interception of the picture at any point without either consent or a court order would be in violation of the statute. By contrast, if law enforcement officials were to install their own cameras and create their own closed circuit television picture of a meeting, the capture of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. This would be so even if the law enforcement agency utilized the wiring in the premises to insall the cameras and transmit the images. Intercepting the audio portion of the meeting would of course be an interception of an oral communication and the statute would apply to that portion.

Under the Fourth Amendment and recent case law in the area, law enforcement authorities are bound to seek a court order based on probable cause to place a closed circuit television camera in premises where there is a reasonable expectation of privacy without at least one party consent. The whole area of closed circuit television is suitable for Congressional action and is a likely subject of legislation in the future. *See* H.R. 3455 (Kastenmeier) (applying Title III standards to video surveillance) The Committee is aware that the Department of Justice follows the rules established by the leading cases in this area in seeking closed circuit television orders,[84] and the Committee believes this is a wise procedure pending either legislation on the subject or a final judicial resolution of these issues.

Subsection (a)(5) also adds a new definition for "electronic communication system" to mean any wire, radio, electronic photoelectronic or photooptical facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Subsection (a)(5) adds a definition for "electronic communication service" to mean any service which provides to users thereof the ability to send or receive electronic communications or wire communications. These services can be provided through the same facilities. Common carriers like existing telephone companies are deemed providers of an electronic communication service.

---

[84] United States v. Torres, 751 F.2d 875 (7th Cir. 1984); see also *United States v. Brasucci*, 786 F. 2d 504 (2d Cir. 1986).

Subsection (a)(5) adds a definition for the term "readily accessible to the general public." This term is used in section 2511(2) which creates an exception to the general prohibitions on interception. The new paragraph (16) states "readily accessible to the general public" means with respect to a radio communication, that such is not in one of five separate categories. In other words, if a radio communication fits into one of the five categories then it will have privacy protection (unless some other exception applies to preclude coverage). The first category of protected communications [85] is radio communications which are scrambled or encrypted. The terms scrambled or encrypted are used in their technical sense. To "Encrypt" or to "Scramble" means to convert plaintext into unintelligible form by means of equipment intended to protect the contents of a communication from unintended recipients. Equipment which merely changes the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide "encryption" within the meaning of this bill. The use of a word code, no matter how sophisticated, would not suffice. Examples of scrambling techniques which are currently available include the data encryption standard (DES).

The second type of protected communications is spread spectrum radio communications. These radio signals are transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication. *See* 50 FED. REG. 25234 (June 18, 1985). Spread spectrum technology usually involves the transmission of a signal on different frequencies and the receiving station must possess the necessary algorithm in order to reassemble the signal.

The third type of protected communications is radio communications carried on a subcarrier or other signal subsidiary. This category includes, for example, data and background music services carried on FM subcarriers and data carried on the vertical blanking interval (VBI) of a television signal. Under Section 2511(2)(g)(ii)(I), however, it is not unlawful to intercept subcarrier and VBI communications that are transmitted for the use of the general public, *e.g.*, the stereo subcarrier used in FM broadcasting, or data carried on the VBI to provide closed-captioning of television programming for the hearing-impaired.

The fourth type of protected communications is those which are carried by common carriers. There is an exception for tone-only paging systems. Thus, the interception of tone-only paging system transmissions will not be prohibited by this law. On the other hand, the unauthorized interception of a displaying paging signal intended for digital display by the paging receiver (which involves the transmission of alphanumeric characters over the radio) carried by a common carrier is illegal.

---

[85] Protected communication as used in this description means that the communication is otherwise legally protected against interception absent the application of some other exception such as one party consent.

The fifth type of protected communications consists of certain types of radio signals. Included in this category are satellite communications, auxiliary broadcast services and private microwave services. Each of these services routinely carries business or personal communications made with an expectation of privacy. These categories are described by reference to certain parts of the Rules of the Federal Communications Commission. This category excludes certain communications which are essentially two-way voice radio communications.

Part 25 of the FCC's Rules regulates communications made by satellite. Such communications are not defined to be readily accessible to the general public. Two other provisions of this Act, however, limit the liability incurred under chapter 119 by the interception of certain types of satellite communications. Section 2511(g)(iii)(II) exempts activities covered by section 705(b) of the Communications Act, relating to the interception or receipt of certain satellite cable programming for private viewing; accordingly, such activities are not unlawful under chapter 119. Section 2511(4)(b)(iii) further provides that it is not an offense under Section 2511(4) to intercept an unscrambled and unencrypted "network feed"—*i.e.*, a satellite transmission that is transmitted to a broadcasting station for purposes of retransmission to the general public—so long as the conduct is not for the purposes of direct or indirect commercial advantage or private financial gain.

Also excluded from the category of readily accessible radio communications are those transmitted on frequencies allocated under subparts D, E, and F of Part 74 of the FCC's Rules. Under the FCC's Rules, these frequencies may be licensed only to broadcasters. 47 C.F.R. §§ 74.432, 74.532, 74.632. Each of the subparts regulates communications that are entirely internal to a broadcast operation. They include, for example, video and audio transmissions from a news team in the field to the studio, and transmission from the studio to the transmitter site. Part 74 transmissions may also include two-way voice communications, such as those between studios and remote crews; but this Act provides an exception for such two-way voice communications made on frequencies shared with services outside Part 74. The interception of communications on such shared frequencies is not unlawful under chapter 119.

The final service excluded from the category of readily accessible radio communications is that regulated under Part 94 of the FCC's Rules, the private operational fixed microwave service. This service carries confidential business data. Under limited conditions, it may also be used to transmit certain types of television material. Transmissions under Part 94 are generally made with the intent of maintaining privacy, and it would be inappropriate to disrupt ongoing business practices by making those communications available to competitors and to other members of the public.

Subsection (a)(5) also provides a definition for "electronic storage". That terms means "any temporary intermediate storage of a communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Section 2510(17) defines "electronic storage" to mean any temporary, intermediate storage of a communication incidental to the electronic transmission thereof, and any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Under Section 2710, computer storage is defined as an element of "remote computing service". These definitions are not intended to limit the terms "electronic storage" or "computer storage" to any particular medium of storage. While storage often takes place within the random access memory of a computer, the term applies equally to storage in any other form, including that on magnetic tape, disks, or other media. Thus, for example, the prohibitions against unauthorized access to a wire or electronic communication while it is in electronic storage, as set forth in Section 2701, would prohibit unauthorized access to such a communication while it is stored on magnetic tape or disk. The prohibitions would apply similarly to information held on magnetic tape or disk pursuant to an agreement to provide remote computing service.

Subsection (a)(5) adds a new definition for the term "aural transfer". "Aural transfer" means a "transfer containing the human voice at any point between and including the point of origin and the point of reception". Under this definition voice messages transferred over a paging system are protected. It is intended that computer-generated or otherwise artificial voices are not included in this definition and thus will not be part of a "wire communication". They would, however, be part of an "electronic communication".

Subsection 101(b) makes three different types of amendments to existing title 18.

Subsection (b)(1) amends section 2511(2)(d) of title 18 by striking out "or for the purpose of committing any other injurious act". Under current federal law it is permissible for one party to consent to the interception and recording of a conversation. This exception to the general prohibition on interception, however, contains an exception relating to persons who intercept or record communications for illegal, tortious or other injurious purposes. This exception was added in 1968 by the late Senator Hart in an effort to prevent one party from intercepting or recording a conversation for blackmail or similar improper purposes. Unfortunately, that floor amendment was not drafted with precision. As a result, numerous court cases have arisen wherein the term "other injurious purposes" has been construed and misconstrued. Most troubling of these cases have been attempts by parties to chill the exercise of First Amendment rights through the use of civil remedies under this chapter. For example, in *Boddie* v. *American Broadcasting Co.*, 731 F.2d 333 (6th Cir. 1984), the plaintiff, whose conversations were recorded by a journalist, sued. Despite the consent of the reporter who was a party to the conversation, the plaintiff claimed that the recordation was illegal because it was done for an improper purpose (e.g., to embarrass the plaintiff). The court's opinion suggests that if the network intended to cause "insult and injury" to plaintiff Boddie, she might be entitled to recover. This interpretation of the statute places a stumbling block in the path of even the most scrupulous journalist. Many news stories have been brought to light by recording a conversation with the consent of only one of the parties involved—often the journalist himself. Unfortunately, many news stories are embarrassing to someone. The present form of the statute not only provides such a person with a right to bring suit, but it also makes the actions of the journalist potentially a criminal offense under section 2511, even if the interception was made for the purpose of committing neither a criminal act nor a tort. The statute thus presents the journalist with a hard choice: to get the news may expose him or her to a criminal conviction and/or civil liability. And whether a journalist is convicted in fact may turn, under *Boddie,* on how a jury sitting years later assesses the journalist's subjective intent. The Committee finds such a threat to be inconsistent with the guarantees of the First Amendment. Inasmuch as the amended statute continues to prohibit interceptions made for the purpose of committing either a crime or a tort (including acts of defamation), the Committee believes that the public will be afforded ample protection against improper or unscrupulous interception. The amendment is intended to remove only the shadow of a finding that section 2511 has been violated by interceptions made in the course of otherwise responsible news gathering. While the appeals court decision merely sent the case back for further factual development, it is clear from the facts of the case that the term "improper purpose" is overly broad and vague. The deletion of the term leaves in place the exception to one party consent for illegal or tortious interceptions or recordation. Thus, the original purpose of the Hart amendment is preserved without maintenance of the litigation-breeding phrase. This amendment is supported by the Department of Justice.

Subsection (b)(2) amends section 2511(2)(f) to expand the exception applicable to foreign intelligence activities to make sure the provisions of chapter 121 do not adversely affect such activities.

Section 101(b)(2) of H.R. 4952 amends section 2511(2)(f) of Title 18 to ensure that nothing in chapter 119 or chapter 121 of Title 18 as amended by H.R. 4952, affects existing legal authority for United States Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

Further the Committee expects that the practice of providing to the House and Senate Intelligence Committees proposed changes in relevant executive branch procedures and regulations governing the conduct of intelligence activities, including those involving electronic surveillance, physical searches, and the minimization of information collected concerning U.S. persons will be continued. As in the past, the Committee expects that any relevant changes in these procedures and regulations will be provided to the intelligence committees prior to their taking effect.

Finally, as has been noted before, since Congress last addressed the issue of privacy of communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically, and are expected to continue to do so. These factors have raised serious issues about the protection of the privacy interests of U.S. citizens, which are of great concern to this Committee and to the American people. For this reason, the Committee wishes to emphasize the obligation of the heads of intelligence agencies to continue to keep the Permanent Select Committee on Intelligence fully and currently informed of all intelligence activities pursuant to Title V of the National Security Act of 1947.

Section 107 of H.R. 4952 emphasizes that nothing in Title I of the bill or the amendments made by Title I, such as the changes made to 18 U.S.C. 2511(2)(f), provides authority for the conduct of any intelligence activity.

Subsection (b)(4) of section 101 of the bill amends section 2511(2) to provide new exemptions from criminal liability which are appropriate to the new types of technologies which are added to the privacy protection of the federal wiretap law. Thus, the bill lists a series of types of interceptions which are permissible.

The Committee has drafted the present Act with an eye to its interplay with Section 705(a) of the Communications Act of 1934. In particular, where this bill provides that "it shall not be unlawful" for the public to engage in specific conduct with respect to radio transmissions, the Committee intends that such a provision does not "authorize" the conduct for purposes of the first sentence of Section 705(a) of the Communications Act. Accordingly, the legality of such conduct remains subject to inquiry under the Communications Act. In contrast, where the bill provides that a specified person "may" engage in certain conduct, or uses similar language in the affirmative, the Committee intends that such a provision does "authorize" the conduct for purposes of Section 705(a). The legality of such conduct would be determined under Title 18. In addition, where judicial interpretations have previously determined that certain types of activities are implicitly authorized for purposes of Section 705, that interpretation is intended to continue in effect. *See, e.g., United States* v. *Freeman*, 524 F.2d 337, 340 (7th Cir. 1975), *cert. denied*, 424 U.S. 920 (1976).

The first exemption is a generic exception. It is permissible to intercept electronic communications made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public. The term "configure" is intended to establish an objective standard of design configuration to begin determining whether a system receives privacy protection. An example of systems which are readily accessible include loud speakers hooked up to a telephone system.

It should be noted that the term "readily accessible to the general public" is a defined term with respect to radio communications. See discussion, at ——, *supra*. Under section 101(b)(4) nothing carried by wire is "readily accessible to the general public".

Nothing in the bill affects the use of radar detectors, because the radar transmissions are readily accessible to the general public. Nothing in the bill, however, affects the authority of states to regulate the use of radar detectors.

The second set of exceptions relate to specific types of radio communications which have traditionally been free from prohibitions on mere interception. Thus, it is permissible to intercept any radio communication which is transmitted (1) by any station for the use of the general public,[86] or that relate to ships, aircraft, vehicles or persons in distress; (2) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public; (3) by a station operating on a frequency assigned to amateur, citizens band or general mobile radio services, or (4) by any marine or aeronautical communications system.

Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems, are certainly not those to which this legislation is aimed. *All* amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Service are exempt from the electronic communications intercept prohibitions of the bill.

It should be noted that amateurs, in performing their public service functions, occasionally utilize communications of other services, such as NOAA weather broadcasts and the like. As such, many amateurs employ "scanner" receivers which are capable of receiving communications of many different radio services (including amateur VHF and UHF communications, typically). The use of, as an example, a multiband radio receiver by a licensed amateur should not subject the amateur to criminal prosecution or harassment in any fashion. Amateurs have legitimate reason to monitor frequencies outside the amateur bands. Many amateurs, for instance, are enrolled in the Military Affiliate Radio System and the Civil Air Patrol, which use frequencies assigned to the Department of Defense. Others are members of the Coast Guard Auxiliary using frequencies in the Maritime Service allocation. Some 30,000 amateurs are part of Skywarn, a system operated by the National Weather Service for tracking and warning of severe weather conditions, e.g., tornadoes; at times it may be required that they monitor Government frequencies in connection with this work. In short, there is legitimate reason for amateurs to have equipment which tunes beyond amateur bands.

The Committee considered listing all the existing radio services which are exempt from the bar on interceptions, but rejected that approach because it would have been cumbersome, possibly redundant, and would have had a built-in obsolescence. When the Committee asked the Federal Communications Commission for a list of radio services which were currently regulated by the FCC of the same kind as those listed in the bill, they provided a list of more than 40 such services. Such a list is extremely lengthy and the nomenclature used is frequently changing. Therefore, instead of listing all of these services the Committee listed some of the more common radio services. In addition, the bill includes a "generic" exception relating to radio services which are "readily accessible to the general public." Thus, for example, private land mobile services (currently licensed under Part 90 of the FCC Rules) are exempt from the prohibition on interceptions.

This subsection also exempts from coverage any conduct which is also prohibited by section 633 of the Communications Act of 1934.

---

[86] These include all communications transmitted for the use of the general public, including radio and television broadcast signals transmitted under Part 73 of the FCC Rules.

Thus, if an individual violates the criminal prohibitions in section 633 (relating to cable piracy) they cannot also be charged under this chapter of title 18.

The subsection also exempts conduct which is excepted from section 705(a) of the Communications Act by virtue of section 705(b) of that Act. Thus, if conduct is permitted under section 705(b) it would not be a crime under this chapter of title 18. Determination of whether conduct is permitted under section 705(b) must, of course, be the result of an examination of the statute, relevant legislative history, existing court interpretations, and constructions given the statute by appropriate federal regulatory entities.

With respect to the interception of radio communications by home satellite dishes, the Committee does not intend to make criminal any type of conduct that is currently lawful under Section 705 of the Communications Act and the present Wiretap Act. To remove any doubts about its impact on home satellite dish owners, H.R. 4952 contains a provision expressly stating that it is not unlawful under Title 18 to intercept unscrambled network programming feeds to affiliates—*i.e.*, communications "transmitted to a broadcasting station for purposes of retransmission to the general public"—unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. Accordingly H.R. 4952 does not create a new class of criminal conduct concerning interception of radio communications by home satellite dishes. In order to violate Title 18, moreover, an interception must be "willful". Incidental or inadvertent interception of a protected video signal which does not benefit a home dish owner would not constitute a criminal violation of the statute. H.R. 4952, in short, is carefully drafted to remain as neutral as possible with respect to the coverage of both Section 705 and Title 18 as to interception of radio signals by home satellite dish owners. "Private gain" is a term defined in section 705(b) and the meaning given there is intended to apply to this section as well.

H.R. 4952 adds a new Section 2511(4)(c) which exempts from Title 18 the reception by home earth station owners of certain unscrambled satellite transmissions, as long as such reception is not for commercial advantage or private gain (including any use by a commercial establishment). While the bill does not make criminal any type of conduct with respect to interception of radio communications by home satellite dishes that is currently lawful under section 705 of the Communications Act and the provisions of Chapter 119 of Title 18, the specific exemption in this subsection does not apply to the interception of private communications via satellite such as sporting events when they are not the final output of a national television network to a broadcasting station for purposes of retransmission to the general public.

However, even the unscrambled satellite transmission which is not protected under Title 18 because it comes within Section 2511(4)(b)(iii) may in fact be a private communication, and H.R. 4952 is not intended to exempt such noncommercial interception from liability, if any, under Section 705 of Title 47 or otherwise "authorize" interception of unscrambled transmissions for noncommercial purposes. Rather, the intention of the Committee is that the legality of noncommercial interception of this type of unscrambled satellite transmission will be decided under Section 705 of the Communications Act. The Committee expresses no view on this issue. The Committee notes, however, that it is the view of the General Counsel of the FCC that interception and viewing by home earth station owners of television network satellite feeds to local affiliated television stations could subject the interceptor to civil and criminal penalties under the Communications Act. *See,* Letter of Jack D. Smith to Honorable Robert Kastenmeier, Chairman, Subcommittee on Courts, Civil Liberties and the Administration of Justice, November 27, 1985. *Compare National Football League* v. *McBee & Benno's,* — F.2d— (8th Cir. June 4, 1986) (individual interception of "clean feeds" not permanently enjoined because of equitable considerations).

[The letter follows:]

FEDERAL COMMUNICATIONS COMMISSION,
Washington, DC, November 27, 1985.

Hon. ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Washington, DC.

DEAR CONGRESSMAN KASTENMEIER: At a recent meeting between congressional and Commission staff, David Beier requested that my office issue an opinion on the applicability of Section 705 of the Communications Act to network television feeds. Specifically, we were asked whether Section 705 prohibits owners of satellite antennas from intercepting the networks' television feeds as they are being distributed to their affiliates via satellite. In general, those transmissions contain network programming and the national commercial spots. Local adveretising and programming are added at the affiliates' broadcast station. Thus, by intercepting the networks' satellite feeds, viewers are seeing essentially the same programs as other television viewers but without certain commercials.

Section 705 provides, in pertinent part that

> No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. . . . This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public.

The courts, in several civil and criminal actions, have been the primary interpreters of Section 705. Unfortunately, none of the decided cases are directly on point in that they do not apply to the interception of satellite network feeds. However, the case law applying Section 705 to MDS transmissions strongly suggests that Section 705(a) prohibits the unauthorized interception of satellite network feeds.

The networks' satellite feeds clearly constitute interstate radio communications. Viewing those transmissions constitutes a use by the owner of the satellite antenna of the signal "for his own benefit". *See e.g., Movie Systems, Inc.* v. *Heller,* 710 F. 2d 492 (8th Cir. 1983); *Hoosier Home Theater, Inc.* v. *Adkins,* 595 F. Supp. 389 (S.D.

Ind. 1984). The networks and their local affiliates fund their operations from advertising revenues, which, in turn, are a function of the size of the viewing audience. Because some local commercials are not carried on the network feeds, owners of satellite antennas would not see those commercials and hence would not generally be counted as part of the viewing audience. Therefore, unauthorized interception of the satellite network feeds has the effect of reducing the networks' audience and, as a consequence, their affiliates' operating revenues. In economic terms, this appears to be analogous to the unauthorized interception of subscription television signals without payment.

Section 705(a) expressly excludes from its prohibition radio communications transmitted for the use of the general public. Satellite transmissions, like MDS transmissions, are, however, a common carrier service provided on common carrier frequencies. *See Movie Systems, Inc.* v. *Heller, supra* at 495; *Home Box Office, Inc.* v. *Advanced Consumer Technology, Movie Antenna, Inc.*, 549 F. Supp. 14, 24 (S.D.N.Y. 1981); *Chartwell Communications Group* v. *Westbrook*, 637 F.2d 459, 465 (6th Cir. 1980). For the reason discussed above concerning advertising revenues, they are not intended to be viewed by the general public in the form they are transmitted from satellites. Additionally, in determining the applicability of this exclusion, the critical factor is the intent of the party transmitting the radio communications. *See Chartwell Communications Group* v. *Westbrook, supra* at 464–465. The networks are of course the ultimate authority on their intent. It appears that network satellite feeds are only intended for reception by their affiliates. We believe that the networks are considering scrambling these transmissions in order to preclude their interception. Existing case precedent does not require, however, that networks scramble their signals in order to be encompassed within Section 705. *See Home Box Office, Inc.* v. *Advanced Consumer Technology, Movie Antenna, Inc., supra* at 21–22; *Hoosier Home Theater, Inc.* v. *Adkins, supra* at 396.

Finally, we recognize that under certain conditions, Section 705(b) further excepts from the prohibition of 705(a) the interception of satellite cable programming for private viewing. The satellite network feeds are not, however, satellite cable programming as that term is defined in Section 705(c)(1). Thus, Section 705(b) does not otherwise sanction the interception.

In summation, Section 705(a) appears to encompass the network satellite feeds. Unauthorized interception of those signals by home owners with satellite antennas or the unauthorized sale of decoders could lead to civil or criminal actions under Section 705. *See e.g., Movie Systems, Inc. v. Heller, supra; United States v. Westbrook*, 502 F. Supp. 588 (E.D. Mich. 1980).

Sincerely yours,

JACK D. SMITH, *General Counsel.*

Subsection (g)(iv) also exempts from the criminal prohibitions the interception of any electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference. This exemption was suggested by the Association of North

American Radio Clubs (ANARC) and meets the needs of the Federal Communications Commission.

Finally, this subsection, (g)(v), exempts the interception of a radio communication which is made for other users of the same frequency when such communication is made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or use of such a system, as long as the communication is not scrambled or encrypted. This exception will permit the monitoring of shared channels on marine radio which utilizes an onshore operator.

Subsection (b)(4) also amends section 2511(2) to add a new subsection (h). Proposed subsection (h)(i) clarifies that this chapter does not regulate the use of pen registers. The new subsection (h)(ii) states that no violation of this chapter occurs if a provider of wire or electronic communication service records the fact that a communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or user of that service, from fraudulent, unlawful or abusive use of such a service. This provision permits the electronic and wire communication providers to protect themselves and their customers. Thus, the Committee continues the current law and practice with respect to activities of telephone companies to protect themselves against fraud, abuse or unlawful use. *See United States* v. *Auler,* 539 F.2d 642 (7th Cir. 1976), *cert. denied,* 429 U.S. 1104 (1977); *United States* v. *Goldstein,* 532 F.2d 1305 (9th Cir.), *cert. denied sub nom. Roberts* v. *United States,* 429 U.S. 960 (1976); *United States* v. *Freeman,* 524 F.2d 337 (7th Cir. 1975), *cert. denied,* 424 U.S. 920 (1976); *United States* v. *Clegg,* 509 F.2d 605 (5th Cir. 1975); *United States* v. *Shah,* 371 F. Supp. 1170 (W.D.Pa. 1974).

Proposed subsection (h)(iii) states that it is not unlawful to use a "trap and trace" device. *See Michigan Bell Tel. Co.* v. *United States,* 585 F.2d 385 (6th Cir. 1977) (upholding the use of trap and trace devices under Federal Rule of Criminal Procedure. Rule 41)

Subsection (c) provides technical and conforming amendments. Subsection (c)(1) adds "electronic communication" in appropriate places throughout the chapter.[87] Subsection (c)(2) amends the heading of the chapter. Subsection (c)(3) amends the table of chapters to add electronic communications to the table. Subsection (c) (4), (5), (6) and (7) makes appropriate technical amendments to delete the term "common carrier" and substitute in its place "provider of wire or electronic communication service."

Section 2511(2)(a)(i), as amended, specifies that it is not unlawful for the employees of providers of wire or electronic communication services to intercept customer communications in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of the service or to the protection of the rights or property of the providor, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality checks. In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order properly to route, terminate, and otherwise manage the individual messages it contains. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited. In contrast, the traditional limits on service "observing" and random "monitoring" do refer to human aural interception and are retained with respect to voice ("wire") communications.

---

[87] Similarly it should be noted that the amendments to section 2511(2)(d) (relating to one—party consent) also apply to private microwave services. It is the Committee's intent to extend the exemption with respect to one—party consent in section 2511(2)(d) to electronic communications. For example, if a licensee of a private microwave system, licensed pursuant to Part 94 of the Federal Communications Commission's Rules, or the operator of a private wireline or private fiber optic system secures consent for the licensee's or operator's recording and/or monitoring of communications over that private system from one of the parties to the communications, such recording and/or monitoring is permissible.

Subsection (d) modifies the general penalty structure for criminal violations of this chapter. The general rule is that a willful violation is punishable as a five year felony. Thus, unless one of the exceptions applies to a person found guilty of willfully violating one of the criminal statutes in the chapter, they will be liable for a fine under the chapter [88] and imprisonment of up to five years or both.

The first exception for this general rule is that the interception of radio communications are punishable as one year misdemeanors, with fines of up to $100,000 18 U.S.C. 3623. There are three exceptions to this general rule. If the offender has been previously found to have been guilty of an offense of intercepting radio communications, then the felony provisions apply. Similarly, if the interception is done for illegal, tortious or commercial gain purposes, then the offender is punishable under the felony penalty. The second exception is that first offenders who intercept the radio portion of a cellular telephone call (and who act without one of the enumerated bad purposes) may only be subject to punishment of up to six months in prison or a $500 fine or both.

In the event that an offender intercepts the wire portion of a telephone call such conduct remains a five year felony.

The third exception is that conduct, otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public, is not an offense under this chapter and is not subject to civil liability, unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. The terms "direct or indirect commercial advantage or private financial gain" are intended to have the same meaning as those terms have when used in 47 U.S.C. 705(b). This third exception decriminalizes the interception of "network feeds" under title 18. The exception does not extend beyond "network feeds." The

---

[88] 18 U.S.C. 3623 provides for a different maximum fine level for felonies, or misdemeanors resulting in death. Individual defendants can be fined up to $250,000 and organizations up to $500,000.

Committee notes that interception and disclosure or use may violate section 705 of the Communications Act. *See* note 9, *supra*.

The penalty structure assumes that more active participation is necessary when a person engages in traditional wiretapping or bugging; therefore, a higher degree of culpability attaches to such conduct. Similarly, higher penalties are justified for second or subsequent offenders or for offenders who engage in prohibited conduct for improper purposes. On the other hand the Committee recognized that although the criminal provisions of the chapter require "willful violations", interception of radio transmissions can be more easily achieved. Therefore, the Committee reduced the penalties for the interception of radio transmissions.

Subsection (e) amends section 2518(10) to provide that the remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions available for non-constitutional violations of this chapter involving such communciations. In the event that there is a violation of law of a constitutional magnitude the court involved in a subsequent criminal trial will apply the existing constitutional law with respect to the exclusionary rule. *Mapp* v. *Ohio*, 367 U.S. 643, 652 (1961); *Massachusetts* v. *Shepperd*, 104 S.Ct. 3424 (1984); *United States* v. *Leon*, 104 S.Ct. 3405 (1984).

Section 102 amends section 2511 of title 18 to add a new criminal prohibition on disclosure by adding a new subsection (3)(A). The new language provides that a person or entity providing wire or electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or the agent of such addressee or intended recipient. The amendment to section 2511 made by § 102 includes the term "to the public" and hereby includes the government as part of the public. Thus, FTS services are included. The term "willfully" is used so as to conform this criminal prohibition with those in the rest of the chapter.

The term "willful" as used in this chapter has been construed—and misconstrued—by the courts. Note, An Analysis of the Term Willfull in Federal Criminal Statutes, 51 NOTRE DAME LAWYER 786 (1976). By retaining the same terminology the Committee does not intend to perpetuate the confusion which has emerged in the case law. See C. Fishman, *Wiretapping and Eavesdropping*, Cum. Suppl. 1985 section 7.15 pages 37–41. Thus, the Committee intends that the term have the same meaning as the term intentional. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" circumstances.

The term "intentional" is narrower than the dictionary definition of "intentional". "Intentional" means more than that one *voluntarily* engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective.

In contrast a knowing state of mind is (1) an awareness of the nature of the conduct, (2) an awareness of or a firm belief in the existence of the circumstance and (3) an awareness of or a firm belief in the substantial certainty of the result.

Thus, the distinction between an "intentional" state of mind and a "knowing" state of mind is narrow but important. As recently stated by Mr. Justice Rehnquist,

> Perhaps the most significant, and most esoteric, distinction drawn by [Model Penal Code] analysis is that between the mental states of "purpose" and "knowledge". As we pointed out in *United States* v. *United States Gypsum Co.*, 438 U.S. 422, 445 (1978), a person who causes a particular result is said to act purposefully (intentionally) "when he consciously desires that result, whatever the likelihood of that result happening from his conduct"; while he is said to act knowingly if he is aware "that the result is practically certain to follow from his conduct, whatever his desire may be as to that result." [footnote omitted.]
>
> In the case of most crimes, "the limited distinction between knowledge and purpose has not been considered important since 'there is good reason for imposing liability whether the defendant desired or merely knew of the practical certainty of the results,'" [citation omitted] * * *

In certain narrow classes of crimes, however, heightened culpability has been thought to merit special attention. *United States* v. *Bailey*, 444 U.S. 394 (1980).

The term "intentional" does not require that the act was committed for a particular purpose or motive. *See* Senate Report 97-307 at 67.

By the use of the term "willful" (throughout chapter 119)—and its accompanying definition—the Committee precludes the applicatin of civil or criminal liability for acts of inadvertent interception.

This section contains an exception to the limitations of divulgence. The exception applies to persons or entities providing wire or electronic communication service to the public. Such persons or entities are permitted to divulge the contents of any such communication if: (1) otherwise authorized in section 2511(2)(A) or 2517 of title 18; (2) with the consent of the originator of any addressee or intended recipient of such communication; (3) to any person employed or authorized, or whose facilities are used, to forward such communication to its destination, or (4) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement agency.

The exceptions to the divulgence bar are relatively straightforward. Obviously providers should be permitted to divulge under other provisions of the chapter. To be consistent with the one party consent exception found in the chapter a similar exception is appropriate here. It is also logical to provide an exception with respect to activities necessary and intrinsic to the communication activity, therefore it is necessary to exempt communication intermediaries. Finally, if a communication provider inadvertently obtains the contents of a communication during transmission which appears to relate to the commission of a crime, divulgence is permitted when such divulgence is made to a law enforcement agency. If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred this exception would not apply.

Section 103 amends—largely by recodifying—the existing section 2520 of title 18 to incorporate violations involving interception, disclosure or willful [89] use of wire, oral or electronic communications. Proposed subsection (a) authorizes the commencement of a civil suit. The plaintiff may bring a civil action under Section 2520 whether or not the defendant has been subject to a criminal prosecution for the acts complained of; but in the absence of such prosecution and conviction, it is the plaintiff's burden to establish that the requirements of this section are met. Subsection (b) indicates that appropriate relief can include: (1) preliminary and other equitable or declaratory relief as may be appropriate; (2) damages and punitive damages; and (3) reasonable attorney's fees and other litigation costs reasonably incurred. Subsection (d) of proposed section 2520 provides a method for the computation of damages. Under subsection (c) the court may assess damages consisting of whichever is greater of the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation or statutory damages of whichever is greater of $100 a day for each day of violation or $10,000.

Subsection (d) provides a good faith defense to actions brought under this section. The term "good faith" as used in this section includes the receipt of a facially valid court order. Thus, the fact that the provider of electronic communication service also has received such a court order, means the provider would be entitled to a dismissal of a civil course of action upon a showing that such provider acted within the scope of the court order.

Subsection (e) of proposed section 2520 provides a statute of limitations for actions brought under this section. The subsection provides that any action may not be commenced later than two years after the date upon which the claimant first has reasonable opportunity to discover the violation.

Section 104 amends the list of federal officials who may make applications for court orders under this chapter. Section 2516(1) is amended to add to the list of officials who may be specifically designated by the Attorey General to authorize applications to include any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division. The addition of an acting Assistant Attorney General is not meant to imply rejection in any other context of the well-established principle that an acting official ordinarily possesses all the legal powers of the official for whom he is acting, *see Keyser v. Hitz,* 133 H.S. 138 (1890), but rather to clarify the law under this statute in light of its unique history and interpretation. *Compare, e.g., United States v. Acon,* 513

---

[89] The term "willful" is intended to have the same meaning as it does when used in other sections of this chapter.

F.2d 513 (3d Cir. 1975), with *United States v. Pellieci,* 504 F.2d 1106 (1st Cir. 1974), *cert. denied,* 413 U.S. 1122.

Section 105 amends section 2516(1) by adding new crimes which can be used to justify an application for wiretapping or bugging order. The new crimes include violation of the following title 18 provisions: (1) section 751 (relating to escape); (2) sections 2312 and 2313 (relating to automobile theft); (3) the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts); (4) section 1203 (relating to fraud and related activities in connection with access devices); (5) felony violations of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain interception devices); (6) section 3146 (relating to penalty for failure to appear); (7) section 3521 (relating to violations of the security of protecting witnesses); (8) section 32 (relating to destruction of aircraft or aircraft facilities); (9) section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire); (10) section 1952B (relating to violent crimes in aid of racketeering activity); (11) section 115 (relating to threats against a federal official); (12) the section in chapter 65 relating to destruction of an energy facility; (13) section 1341 (relating to mail fraud); and (14) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain intercepting devices). In addition, this section authorizes the application for orders under this chapter for the location of a fugitive from an offense described in this section.

Section 105(b) amends section 2516 to authorize the government to apply for a court order authorizing or approving the interception of an electronic communication by an investigative or law enforcement officer when an interception may provide evidence of a federal felony. Thus, for non-wire, non-oral electronic communications, a different and less restrictive list of crimes can be used to justify an application for interception. Section 105(b) permits the government to make applications for the interception of electronic communications. The Committee has been informed by the Department of Justice that for the three years which follow the date of enactment of this legislation that this exercise of authority will only be made pursuant to the approval of the same level of officials as those involved in the approval of applications for wire intercepts. In addition to this voluntary regulatory limitation, the Department of Justice has committed themselves to submit to the relevant Congressional committees any proposed changes in these regulations at least 90 days in advance of any change.

Section 106 contains four subsections. Subsection (a) provides that a court can authorize an order within the court's jurisdiction and outside that jurisdiction but within the United States in the case of a mobile interception device authorized within such jurisdiction. In the usual case the court will authorize the installation of a device, the device will be installed within the court's jurisdiction and the suspect will then move outside the court's jurisdiction. Nothing in this section affects the current law with respect to the use of such devices outside the United States. In certain cases a device authorized for installation, for instance, in an automobile may be authorized in one district and the vehicle might be moved to another district prior to installation. The authorization will permit installation in the district to which the vehicle has been moved.

Subsection (b) amends section 2518(4) by striking out "at reasonable rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance." This is designed to permit reimbursement to be available at an appropriate amount in light of the work required for a particular activity. While in the ordinary case a flat or general rate may be appropriate, this change will permit flexibility to permit reimbursement at a higher level in unusual cases.

Subsection (c) makes two changes in section 2518(5) of title 18. Subparagraph (1) provides a rule for when the 30 days to install a tap or bug begins to run. Under this rule the 30 day time period commences on the earlier of the day on which the officer first begins to conduct an interception or ten days after the order is entered. Under this rule if an officer took 9 days after the entry of the order to effectuate the tap and began to overhear conversations then the 30 day time period would start from on the 9th day.

Subparagraph (2) of subsection (c) of section 106 of the bill provides a special minimization rule. Under this rule when an intercepted communication is in a code or foreign language and an expert in that foreign language or code is not reasonably available during that interception period, minimization may be accomplished as soon as practicable after the interception. In this regard, it is contemplated that the translator or decoder will listen to the tapes of an interception and make available to the investigators the minimized portions preserving the rest for later possible court perusal.

Subparagraph (2) of subsection (c) of section 106 of the bill also provides that the monitoring of interceptions under this chapter may be conducted in whole or in part by Government personnel, or by individuals operating under contract with the Government, as long as such personnel are acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. This change, which was sought by the Federal Bureau of Investigation, is designed to free field agents from the relatively routine activity of monitoring interceptions so that they can engage in other law enforcement activities.

Subsection (d) of section 106 amends 2518 of title 18 to provide new rules with respect to the specificity required in the descriptions of the place to be bugged or tapped. Under current law, the application and the order must indicate the "particular" facility or place in which the interception is to occur. The amendments establish two largely similar rules, the specificity with which the locale of an interception of "oral communications" and "wire communications" can occur.

With respect to "oral communications" a limited list of federal officials can apply for a special order seeking relief under this provision. The application must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are being intercepted. The judge in turn must find that the ordinary specification rules are not practical. Examples of situations where ordinary specification rules would not be practical would be a suspect who moves from room to room in a hotel to avoid a bug and who sets up a meeting with another suspect for a beach or field. In that case, the order could indicate authority to follow the suspect and engage in the interception once the targeted conversation occurs.

The rule with respect to "wire communications" is somewhat similar. An application for relief from the ordinary specificity rules must be made by a limited list of federal officials. The application must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. Alternatively, a person whose telephone calls were intercepted who said that they were planning on moving from phone to phone or to a pay phone, to avoid detection would have demonstrated that purpose.

Both with respect to "wire" and "dral" communications, where the federal government has been successful in obtaining this relaxed specificity order the government cannot commence the interception until the facilities or place from which the communication is to be commenced is ascertained by the person implementing the interception order. In other words the actual interception could not commence until the suspect commences or evidences an intention to commence a conversation. Thus, it would be improper to use this expanded specificity order to tap a series of telephones, intercept all conversation over such phones and then minimize the conversations collected as a result. This provision puts the burden on the investigatory agency to ascertain when the interception to take place.

Section 107 subsection (a) provides that "* * * (n)othing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity. This provision clarifies that the amendments made in section 102(b)(3) are not read as constituting any new authority; rather those amendments represent an exemption from this chapter and chapter 121 for otherwise lawful activities.

Section 107(b)(1) exempts communications security monitoring from coverage by Chapter 119 or 121 of Title 18, United States Code. Communications security measures are protective measures taken to deny unauthorized persons information derived from United States Government telecommunications and to ensure the authenticity of such communications. Communications security protection results from the application of security measures to electrical systems generating, handling, processing, or using information the loss of which could adversely affect the national interest. Communications security monitoring is the systematic examination of telecommunications carried out to determine the adequacy of communications security deficiencies, to provide data from which to predict the effectiveness of proposed communications security measures, and to confirm the adequacy of such measures after implementation. Communications security monitoring is an essential part of such examinations and is conducted pursuant to detailed guidelines approved by the Attorney General. *Supra,* note 11. These procedures generally set forth an elaborate procedure to assure the communications security monitoring of private communications (as defined in para. 4.e.) is based on consent. *See* para. 5.b. and 6.e. of NASCI, 4000A. Communications security monitoring is the act of listening to, copying, or recording transmissions of the Executive Branch official telecommunications, including the communications of certain contractors, to provide technical material for analysis in order to determine the degree of security being provided to these transmissions. This security, includes, for example, that provided by cryptographic equipment. For purposes of communications security monitoring, government telecommunications are telecommunications of any employee, officer, contractor, or other entity of the United States Government which concern an official purpose of government and which are transmitted over a telecommunications system owned or leased by the United States Government or a Government contractor.

Subsection (b) of section 107 provides that this Act does not affect the conduct by officers and employees of the United States Government when such conduct is in accordance with other applicable federal law and if conducted in accordance with procedures approved by the Attorney General. *See e.g.,* Letter from William French Smith, Attorney General, to Lincoln D. Faurer, Director, National Security Agency, dated January 9, 1984 (relating to Guidelines For the Conduct of Communications Security Monitoring Activities, NACSI No. 4000A). The type of activity referred to in this proviso relates to one or more of three categories of activities: (1) interception of encrypted or scrambled or other official communications for communications security of United States Executive Branch department or entities or United States government contractors[90]; (2) interception of radio communications transmitted between or among foreign powers or agents of foreign powers; or (3) accessing electronic communication systems used exclusively by a foreign power or an agent of a foreign power.

[The letter follows:]

OFFICE OF THE ATTORNEY GENERAL,
Washington, DC., January 9, 1984.

LINCOLN D. FAURER,
Lieutenant General, USAF,
Director, National Security Agency,
Ft. George G. Meade, MD.

DEAR DIRECTOR FAURER: The attached procedures governing the communications security (COMSEC) activities of the United States government meet the requirements of Executive Order 12333 and are otherwise lawful. Accordingly, they are hereby approved.

---

[90] Government contractor means an individual, corporation, partnership or other entity performing work under a United States Government contract.

[Paragraph regarding internal policy discussions unrelated to lawfulness of the procedures deleted.]

Sincerely,

WILLIAM FRENCH SMITH,
Attorney General.

Attachments.

NACSI NO. 4000

GUIDELINES FOR THE CONDUCT OF COMMUNICATIONS SECURITY MONITORING ACTIVITIES

1. REFERENCES

a. Communications Act of 1934, Public Law 73-416 (as amended).

b. Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351 (as amended).

c. Foreign Intelligence Surveillance Act of 1978, Public Law 95-511.

d. National Communications Security Directive, dated 20 June 1979.

e. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

2. INTRODUCTION

The basic purpose of communications security (COMSEC) monitoring is to provide unique material, not readily available through other sources, to evaluate the status of U.S. COMSEC. The information collected through the COMSEC monitoring program is similar to the information potentially available to foreign powers through their own signals intelligence (SIGINT) collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide a comprehensive data base for analysis. COMSEC monitoring is, therefore, used to provide the empirical data necessary to conduct comprehensive analyses of these vulnerabilities and afford a basis for correcting them.

3. PURPOSE AND SCOPE

a. This Instruction provides policy and guidance for the establishment of COMSEC monitoring procedures consistent with applicable law and regulations.* It implements that portion of the National Communications Security Directive (Reference d.) which assigns the Director, National Security Agency (NSA), responsibility to issue guilelines for the conduct of COMSEC monitoring.

b. This Instruction is applicable to all Federal Government departments and agencies engaged in or using the results of COMSEC monitoring. It has been approved by the Attorney General.

---

* Although there are no Federal statutes specifically addressing COMSEC, References a., b., and c. will have an impact upon any COMSEC monitoring guidelines and procedures.

c. Technical surveillance countermeasures, electronic sweeps, surveillance of non-communications emissions (e.g., radar), and TEMPEST testing are not within the scope of this Instruction.

4. DEFINITIONS

a. *COMSEC.* Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials.

b. *COMSEC Monitoring.* The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions.

c. *Contents.* When used with respect to a communication, it includes any information concerning the identity of the parties thereto, or the existence or meaning of that communication.

d. *Electronic Surveillance.* The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

e. *Private Communication.* A communication in which the parties thereto, in the absence of their consent to be monitored for COMSEC purposes, have a reasonable expectation of privacy.

f. *Telecommunications.* The transmission, communication, or processing of information, including the preparation of such information therefor, by electrical, electromagnetic, electromechanical, or electro-optical means.

g. *Telecommunications System.* The devices used to transmit and/or receive communications or process telecommunications, including the preparation of information, therefor; the devices may be electrical, electromagnetic, electromechanical, or electro-optical.

h. *Government Telecommunications.* Telecommunications of any employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a Government contractor. (See Telecommunications and Telecommunications System, above.)

5. POLICY

a. The Government will conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to Government telecommunications and aid in countering their vulnerability. Such activities shall be conducted in strict compliance with current law, executive orders, and policy.

b. Government telecommunications systems are subject to COMSEC monitoring by duly authorized Government entities. The use of such systems by any person shall be construed to imply consent to the monitoring for COMSEC purposes of communications carried over them.** Users of these systems must be properly notified in advance, in accordance with the guidelines in subparagraph 6.e., below, that their use of these systems constitutes consent to monitoring for COMSEC purposes. The Government shall not monitor telecommunications systems which are owned or leased by Government contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization (or his designee) and the written opinion of the General Counsel of the department or agency which is conducting the monitoring that procedures, such as those contained in subparagraph 6.e., below, have been implemented sufficiently to afford adequate notice to the contractor organization's employees.

c. The Government shall not monitor for COMSEC purposes the contents of any telecommunication when such monitoring would constitute electronic surveillance.

d. In accordance with procedures approved by the Attorney General, information acquired incidentally from Government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction. When taking such action, the General Counsel of the department or agency which is conducting the COMSEC monitoring shall be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the General Counsel of the department or agency which performed the monitoring.

e. The results of COMSEC monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Reference e. However, the results of COMSEC monitoring of U.S. and Allied military exercise communications may be used for exercise intelligence purposes under procedures prescribed in applicable directives.

f. No department or agency may monitor the telecommunications of another department or agency for COMSEC purposes without the express prior written approval of a responsible official of the department or agency to be monitored, except as provided for in subparagraph 8.b.(2).

g. It is recognized that COMSEC monitoring operations conducted in a crowded telecommunications environment may result in the temporary acquisition of private communications. COMSEC monitoring shall be conducted in accordance with operational procedures which minimize the possibility that the contents of such telecommunications will be acquired. Such procedures shall be consistent with the guidelines contained herein and shall be endorsed by the General Counsel of the department or agency issuing the procedures.

** Consent to COMSEC monitoring is required of only one party to a conversation or transmission.

6. GUIDELINES FOR THE CONDUCT OF COMSEC MONITORING

a. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 2., above:

(1) To collect operational signals needed to measure the degree of security being achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

(2) To provide a basis from which to assess the types and value of information subject to loss through intercept and exploitation of Government telecommunications.

(3) To provide an empirical basis for improving the security of Government telecommunications against SIGINT exploitation.

(4) To assist in determining the effectiveness of Electronic Countermeasures/Electronic Counter-Countermeasures (ECM/ECCM) and cover and deception measures.

(5) To identify Government telecommunication signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide SIGINT elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

(6) To provide empirical data to train users of Government telecommunications systems in proper COMSEC techniques and measures.

(7) To evaluate the effectiveness of COMSEC education and training programs.

(8) To train personnel and to test the capability of COMSEC monitoring equipment.

b. The following categories of telecommunications are not considered private for purposes of this Instruction. Accordingly, acquisition of the contents of any communications in these categories which may occur in the course of locating or examining Government telecommunications is not electronic surveillance.

(1) Commercial broadcast radio communications.

(2) Public safety, citizens band, amateur radio, and similar radio systems licensed by the Government for public use or access.

(3) Any communications in portions of the electromagnetic spectrum which are allocated by the Government for its own use.

c. No incidentally acquired private communication may be monitored beyond the point where a determination can reasonably be made that it is private. A record of the acquisition may be kept for signal identification and avoidance purposes; such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the contents of the communication.

d. Contents of any private communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a Government communication.

e. Notice of the existince of COMSEC monitoring in conformance with subparagraph 5.b., above, can be accomplished by any of the following means or any combination thereof which the legal counsel of the affected department or agency considers legally sufficient to achieve proper notification in terms of content, prominence, and specificity.

(1) Decals placed on the transmitting or receiving devices.

(2) A notice in the daily bulletin or similar medium.

(3) A specific memoradum to users.

(4) A statement on the cover of the official telephone book or communications directory.

(5) A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

7. CONTROL OF MONITORING RECORDS AND EQUIPMENT

a. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or material produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least confidential and downgraded to unclassified when security weaknesses are corrected.

b. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes except as provided for in subparagraph 5.d., above. These reports shall not contain any information extraneous to COMSEC purposes, or names of individuals or sufficient data to identify the source except in an official capacity; e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

c. All COMSEC monitoring recordings and written records, logs, and notes shall be destroyed as soon as operationally feasible.

d. Except as provided for in subparagraph 5.d., above, no information extraneous to COMSEC purposes will be recorded, reported, noted, logged, or filed. If within the capabilities of COMSEC monitoring equipment, any such information that is inadvertently acquired shall be expunged upon recognition. All monitoring records shall be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

e. Access to and dissemination of COMSEC monitoring recordings or written records, reports, logs, and notes shall be limited to that which is necessary for COMSEC purposes. No access to, or dissemination of, such materials beyond COMSEC operational elements shall be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

f. COMSEC monitoring equipment systems shall be safeguarded to prevent unauthorized access and use.

8. RESPONSIBILITIES

a. Heads of departments and agencies shall:

(1) Provide for and conduct COMSEC monitoring operations as they deem appropriate, subject to the provisions of law, executive orders, policy, and this Instruction.

(2) Develop procedures for the conduct of COMSEC monitoring, consistent with the policy and guidelines herein, in col-

laboration with the Director, NSA. Such procedures shall be approved by the Attorney General.

b. The Director, NSA shall:

(1) Advise and assist other departments and agencies in establishing their operating procedures to implement this Instruction.

(2) Monitor fielded Government cryptography as necessary to discharge his responsibilities under the National COMSEC Directive, provided that prior notice will be given to the organization whose encrypted telecommunications are to be monitored. No monitoring will be conducted which results in or affords a substantial likelihood that the plaintext of a communication, other than short-duration plaintext operator conversations associated with establishing a secure condition, will be acquired without the prior approval of the entity whose telecommunications are to be monitored.

LINCOLN D. FAURER,
Lieutenant General, USAF, Director.

Section 108 contains three subsections. Subsection (a) amends chapter 205 of title 18 to add a new section 3117. This section provides that if a court is authorized to issue a warrant or other order for the installation of a mobile tracking device, such an order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction. It should be noted that, unlike a mobile interception device, a tracking device may be utilized outside the United States once the device is installed within the court's jurisdiction. Subsection (b) of the proposed section contains a definition. "Tracking device" is defined to mean an electronic or mechanical device which permits the tracking of the movement of a person or subject.

Subsection (b) of section 108 contains a technical amendment to amend the table of chapters.

The provisions of this section are intended to permit the installation of tracking devices which may move from district to district. The section does not affect the legal standard for the issuance of orders authorizing the installation of each device. *See generally United States v. Karo*, 104 S. Ct. 3296 (1984) (a search warrant not required where the owner consents to installation); *United States v. Knotts*, 460 U.S. 276 (1983) (installation of a beeper on a container to follow on a public roadway does not violate the Fourth Amendment). The Court in *Karo, supra*, did find that if investigators used a beeper to determine whether the beepered object is in a private location, a warrant is required. *See Fishman, Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered*, 34 CATH. UNIV. L. REV. 277 (1985).

Section 109 adds two new offenses to section 2232 of title 18. The first new offense is to warn or give notice to a person that they are the subject of an act of interception under title 18. The elements of the offense require that the defendant have knowledge [91] that the federal law enforcement or investigative officer has been authorized or has applied for an interception order. The defendant need not know that such an application was under a particular chapter of federal law, rather, only that such application or order was under federal law. The defendant must engage in conduct of giving notice of the possible interception to the person who was or is the subject of the interception. *See* House Report 96-1396 at 32-36. Finally, the defendant must be shown to have engaged in such conduct with a specific motive such as to obstruct, impede or prevent the interception. Finally, the offense also includes attempts to engage in the offense.

---

[91] See House Report 96-1396, *Criminal Code Revision Act of 1980*, at 32-36.

The penalty for a violation of this new offense is a possible prison term of up to five years, a fine under this title, or both.

The second new offense set forth in section 109 is to warn the subject of an act of electronic surveillance under the Foreign Intelligence Surveillance Act (FISA). The elements of the offense are identical except that that type of surveillance order is governed by a different statute (FISA) and that statute authorizes a slightly different type of surveillance activity. The penalties for this offense are the same as the aforementioned offense.

Section 110 provides a new section 2521 in title 18. This new section adds to the existing panoply of criminal and civil remedies by authorizing the Attorney General to obtain an injunction to prevent felony level violations of this chapter. This provision is modelled after a similar statute (injunctions against fraud) enacted by Congress in the Comprehensive Crime Control Act of 1984, Public Law 98-473, *see also* Senate Report 97-307 at 1267. This section directs the court to proceed as soon as practicable to the hearing and determination of the matter. This section also provides that preliminary relief can be granted to prevent injury during the pendency of the action. A proceeding under this section is governed by the Federal Rules of Civil Procedure (particularly Rule 65). In the event, however, that an indictment has been returned against the respondent then discovery by both sides is limited to that permissible under the Federal Rules of Criminal Procedure.

Section 111 provides the effective date for the amendments made by this title. Subsection (a) of this section provides the general rule, that except as provided in subsection (b) the amendments made in this title take effect 90 days after the date of enactment. In the case of conduct pursuant to a court order or extension such amendments only apply with respect to court orders or extensions made after this title takes effect. The exception found in subsection (a) is written to permit the continuation under the old law rules of interceptions authorized under such rules. Because ongoing investigations may involve lengthy interceptions, any new order or extension of an order made after the general effective date will be governed by the new law rules.

Subsection (b) of section 111 provides a special rule for state authorization of interceptions. This special effective date rule is necessary because the provisions of chapter 119 of title 18 supersede previous state laws, to the extent that they exist, with respect to electronic communications. Under the provisions of chapter 119 the various states must enact statutes which are at least as restrictive as the provisions of chapter 119 before they can authorize their state courts to enter such interception orders. Because of the massive number of changes made in chapter 119 by this title in relation to electronic communication, it seemed appropriate to grant the states sufficient time to modify their laws accordingly. The special rule, in essence, gives the states two years to bring their laws into conformity with these amendments of chapter 119 of title 18. It is possible that state laws will not need be changed to accommodate revisions on interceptions of wire or oral communications. Any such changes would also benefit from the two-year delayed effective date.

TITLE II—STORED AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORD ACCESS

Section 201 amends title 18 by adding a new chapter 121 which consists of ten new proposed sections. These sections are discussed below.

Proposed section 2701 provides a new criminal offense. The offense consists of either: (1) intentionally accessing, without authorization, a facility through which an electronic communication service is provided or (2) intentionally exceeding the authorization of such facility. In addition, the offense requires that the offender must, as a result of such conduct, obtain, alter or prevent unauthorized access to a wire or electronic communication while it is in electronic storage in such a system. The term "electronic storage" is defined in section 2510(17) of title 18. Electronic storage means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of back-up protection of such communication.

Section 2701(a) makes it an offense intentionally to access without authorization, or to exceed an authorization to access, an electronic communication service and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system. This provision addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public. The Committee recognizes, however, that some electronic communication services offer specific features, sometimes known as computer "electronic bulletin boards," through which interested persons may communicate openly with the public to exchange computer programs in the public domain and other types of information that may be distributed without legal constraint.

It is not the Committee's intent to hinder the development or use of "electronic bulletin boards" or other comparable services. The Committee believes that where communications are readily accessible to the general public, the sender has, for purposes of Section 2701(a), extended an "authorization" to the public to access those communications. A person may reasonably conclude that a communication is readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. To access a communication on such a system should not be a violation of the law.

Some communication systems offer a mixture of services some, such as bulletin boards, which may be readily accessible to the general public, while others—such as electronic mail—may be intended to be confidential. Such a system typically has two or more distinct levels of security. A user may be able to access electronic bulletin boards and the like merely with a password he assigns to himself, while access to such features as electronic mail ordinarily entails a higher level of security (i.e., the mail must be addressed to the user to be accessible specifically). Section 2701 would apply differently to the different services. Those wire or electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public.

Section 2701(a) generally prohibits any person from intentionally accessing a wire or electronic communication system without authorization or in excess of authorization, and thereby obtaining access to a wire or electronic communication while it is in electronic storage in the system. An "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701. A "voice mail" service operates in much the same way, except that the stored message takes the form of the sender's voice, usually in digital code. It would likewise be subject to Section 2701. Similarly, to the extent that a remote computing service is provided through an Electronic Communication Service, then such service is also protected.

A person found guilty of this new offense is subject to a maximum penalty as specified in subsection (b) of proposed section 2701. Subsection (b) provides a general rule that such an offense is punishable by a fine of $5,000 or imprisonment of not more than six months, or both. There are two exceptions to this general rule. If the offender has acted for purposes of commercial advantage, malicious destruction or damage, or private financial gain, the possible penalty is escalated to a fine of up to $250,000 and a prison term of up to one year or both. The second exception is to increase the potential jail term for second or subsequent offenders up to two years in prison.

In light of the importance of communications generally to interstate and foreign commerce, the prevention of unauthorized access to the systems used for such communication is a legitimate federal concern. In some instances, unauthorized access to wire or electronic communications is undertaken for purposes of malice or financial advantage. Other instances, however, arise from the activities of computer amateurs, often called "hackers," whose goal is primarily the access itself. Still, "hacking" cannot be dismissed as a harmless prank; a hacker may stumble across sensitive or commercially useful information, and in any event invades the privacy of those whose communications are stored. It is thus important to prohibit unauthorized access even if undertaken without a malicious purpose or motive. Section 2701(b)(1) does, however, specify higher penalties for unauthorized access committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.

Subsection (c) of proposed section 2701 provides that this section does not apply with respect to conduct which is authorized by: (1) the provider of the service; (2) the user of the service; or (3) the provisions of sections 2703 or 2704 of this new chapter.

Proposed section 2702 provides general prohibitions on the disclosure of contents. This proposed section provides that a person or entity providing electronic communication services to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service. This prohibition is similar to that found in chapter 119 with respect to the divulgence of a wire or electronic communication during transmission. The term knowingly means that the defendant was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness of or a firm belief about the substantial certainty of the result. The conduct in question is the act of disclosure. The result is that the contents have been provided to another person or entity. The circumstances involved are that the person involved provides electronic communication services to the public and that the contents relate to a wire or electronic communication. Knowledge as to a circumstance includes willful blindness, *Model Penal Code* section 2.02. Comment at 129–30 (Tent. Draft No. 4, 1955); *United States* v. *Jewell,* 532 F.2d 697 (9th Cir.), *cert. denied,* 426 U.S. 951 (1976). The concept of "knowingly" does not include, however, "reckless" or "negligent" conduct. *See* House Report 96–1396 at 33–34 (for a definition of terms). This provision is aimed at proscribing the disclosure of stored wire and electronic communications. Subsection (b) contains the exceptions to this general rule.

Subsection (a)(2) of proposed section 2702 provides that a person or entity providing remote computing services to the public shall not knowingly divulge the contents of any communication which is carried or maintained on that service if certain conditions are met. The term "contents" as used in section 2702 is intended to encompass the substance, purport, effect or meaning of the communication. Under this interpretation, a service provider is allowed to divulge mailing lists that identify persons fitting broad demographic criteria. Unless otherwise authorized, service providers may not divulge to third parties information that profiles the activities of individual subscribers through the divulgence of the contents of a communication. The first condition is that the affected communication must be on behalf of and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from) a subscriber or customer of such service. The second condition is that the affected communication be solely for the purpose of providing storage or computer processing services to such subscriber or customer, so long as the provider is *not* authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. The prohibitions of this subsection are also modified by the exceptions in subsection (b).

Section 2702(a) protects communications "received by means of electronic transmission from * * * a subscriber or customer of such service" and kept "solely for the purpose of providing storage or computer processing services to such subscriber or customer * * *." In the case of either electronic mail or voice mail, the sender—a user of the service—has necessarily authorized the addressee's access to the message. The addressee's acquisition of the message is therefore clearly within the contemplation of section 2701(c). Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

Section 2702(a) generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient of such communication, or an agent of such addressee or intended recipient. Similarly, section 2511(3) of title 18, as amended, prohibits such a provider from divulging the contents of a communication while it is in transmission. Neither provision, however, nor any other provision in the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act.

The application of sections 2701(a) and 2511(3) is limited to providers of wire or electronic communications services. There are instances, however, in which a person or entity both acts as a provider of such services and also offers other services to the public. In some such situations, the bill may allow disclosure while another federal requirement, applicable to the person or entity in another of its roles, prohibits disclosure. The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure.

One example of such an instance could arise under the Fair Credit Reporting Act, 15 U.S.C. 1681b, which limits the circumstances under which consumer reporting agencies may disclose certain information relating to consumers. An entity may perform a consumer reporting agency function, and may also provide wire or electronic communication services to the public. Such an entity might provide itself with electronic communication services, including the storage of data relating to consumers. Sections 2701(a) and 2511(3) have no effect on the entity's role as a consumer reporting agency, and in that role the entity must comply with the disclosure limitations of the Fair Credit Reporting Act.

Section 2702(a)(2) prohibits the provider of a remote computing service to the public from knowingly divulging the contents of any communication carried or maintained on the service on behalf of, and received by means of (or created from communications received by means of) electronic transmission from a subscriber or customer of the service. and carried or maintained solely for the purpose of providing such service to the subscriber or customer. This provision reflects the rapidly growing importance of information storage and processing to the Nation's commerce. Today, the subject matter of commerce increasingly is information in electronic form and the processing of information itself has become a major industry. The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records. Accordingly, where an electronic communication is transmitted by a subscriber or customer to such a service, and is stored on the subscriber's behalf solely for the purpose of providing storage or computer processing services to the subscriber, the Committee intends that the communication—together with the products of any processing that the service performs for the customer—remain available only to the subscriber and to the persons he designates, with certain exceptions enumerated in Section 2702(b).

Section 2702 specifies that a person or entity providing wire or electronic communication service to the public may divulge the contents of a communication while in electronic storage by that service with the lawful consent of the originator or any addressee or intended recipient of such communication. The Committee emphasizes that "lawful consent," in this context, need not take the form of a formal written document of consent. A grant of consent electronically would protect the service provider from liability for disclosure under Section 2702. Under various circumstances, consent might be inferred to have arisen from a course of dealing between the service provider and the customer or subscriber—*e.g.*, where a history of transactions between the parties offers a basis for a reasonable understanding that a consent to disclosure attaches to a particular class of communications. Consent may also flow from a user having had a reasonable basis for knowing that disclosure or use may be made with respect to a communication, and having taken action that evidences acquiescence to such disclosure or use—*e.g.*, continued use of such an electronic communication system. Another type of implied consent might be inferred from the very nature of the electronic transaction. For example, a subscriber who places a communication on a computer "electronic bulletin board," with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication. If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.

Section 2702(a) specifies that a person or entity providing a wire or electronic communication service or remote computing services to the public shall not knowingly divulge the contents of any communication while in electronic storage by that service to any person or entity other than the addressee or intended recipient of such communication or an agent of such addressee or intended recipient. Under Section 2702(b), disclosure to any other person requires the consent of the originator or any addressee or intended recipient of the communication. Under some circumstances, however, a customer of or subscriber to a wire or electronic communication service may place a communication on the service without specifying an addressee. The Committee intends, in that situation, that the communication at a minimum be deemed addressed to the service provider for purposes of Section 2702(b). Because an addressee may consent to the disclosure of a communication to any other person, a service provider or system operator, as imputed addressee, may disclose the contents of an unaddressed communication.

A person may be an "intended recipient" of a communication, for purposes of Section 2702, even if he is not individually identified by name or otherwise. A communication may be addressed to the members of a group, for example. In the case of an electronic bulletin board, for instance, a communication might be directed to all members of a previously formed "special interest group" or, alternatively, to all members of the public who are interested in a particular topic of discussion. In such an instance, the service provider would not be liable for disclosure to any person who might reasonably be considered to fall in the class of intended recipients.

Subsection (b) of proposed section 2702 provides six distinct exceptions to the general limitations on divulgence contained in subsection (a). The first exception is with respect to divulgence to an addressee or intended recipient of a communication or an agent thereof. Section 2702(b) which places limits on disclosure. In connection with disclosures made pursuant to section 2702(b)(4), these limitations apply along the agent claim, the second exception is divulgence authorized by statutory provisions in either chapter 119 or this chapter. The third exception is divulgence with the lawful consent of the originator, addressee, or intended recipient (or subscriber in the case of remote computer service). The fourth exception is to permit divulgence to a person who is involved in forwarding the communication to its destination. The fifth exception permits divulgence necessarily incident to the rendition of such services or to the protection of the rights or property of the provider of the services. The terms "rights" and "property" here refer to such rights as intellectual property rights, the right to be free from the theft of services. The term is not intended to be read as to permit a provider to contract with an unauthorized party an obligation to divulge all stored messages, without notice to or any consent from the originator of the message, and then to claim that such divulgence is to protect the rights in such a contract. The sixth exception authorizes the divulgence to a law enforcement agency if the contents of the communication were inadvertently obtained and appear to pertain to the commission of a crime. This exception is intended to be read narrowly. A systematic practice of reviewing stored communications to look for evidence of a crime could not qualify as inadvertent.

Proposed section 2703 contains the procedural requirements for the government to obtain access to electronic communications in storage and transactional records relating thereto. Proposed section 2703 contains four subsections.

Subsection (a) sets forth the requirements which must be met before the government may obtain access to the contents of a nonvoice wire communication or an electronic communication in storage. As a general rule the government must obtain a search warrant. The contents of the voice portion of a wire communication in storage such as with "voice mail" may not be obtained under this section. Under the provisions of chapter 119 of title 18 apply. The general rule applies to electronic communications which have been in electronic storage for 180 days or less. The government is, however, permitted to use alternative means of obtaining access if the communication has been in storage for more than 180 days. For this second category of stored records, the government may use an administrative subpoena authorized by federal or state law or a federal or state grand jury subpoena or a court order under subsection (d) of this section, provided that the customer obtains notice. There is an exception for the notice required for this alternative means, and that exception is set forth in proposed section 2704.

The Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment. The reasons for such a conclusion are set forth more completely earlier in this report. The Committee recognized that electronically stored communications can be of two types. The first type of stored communications are those associated with transmission and incident thereto. The second type of storage is of a back-up variety. Back up protection preserves the integrity of the electronic communications system and to some extent preserves the property of the users of such a system. Most—if not all—electronic communications systems (such as electronic mail systems), however, only keep copies of messages for a few months. To the extent that the record is kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.

Subsection (b) sets forth the procedures the government must use before it can obtain access to the contents of any electronic communication held by a provider of remote computing services. The government may proceed using any of three alternative means of access. The government may, without providing the required notice to the subscriber or customer, obtain a search warrant. The government may also choose to obtain access by giving notice to the subscriber or customer, and using either (a) an administrative summons authorized by federal or state law or a grand jury subpoena; or (2) a court order under subsection (d). The requirement that the state law authorize the use of a grand jury subpoena or administrative summons for purposes of obtaining access to such records—and the parallel requirement in subsection (d) that a court order be obtained under certain standards—are intended to apply the relevant state law with respect to the legal standard such officials must meet with respect to access to those records. Thus, to the extent that a state law or State Constitution requires that a court order based on a standard other than relevance be obtained by a state government official before such official can obtain access to the type of records protected by this chapter, then that law would preclude the use of the provisions of this section with respect to state government officials. Thus, state laws such as those found in Colorado, California, New Jersey and Pennsylvania would remain unaffected with respect to access by state government officials. *See* discussion of records access, *supra*. To the extent that such access is sought by a federal official under the conditions specified under this section, then state law is overridden by virtue of the Supremacy Clause. Examples of such federal legal authority include administrative summons used by the Drug Enforcement Administration, 21 U.S.C. 876, and by the Internal Revenue Service, 26 U.S.C. 7609. Nothing in this authorization eliminates any notice which may be required under other laws. *See, e.g.,* 26 U.S. 7609. The notice required under subsection (b)(1)(B) (i) and (ii) may be dispensed with if the conditions of section 2704 have been met. The type of records to which the provisions of subsection (b) apply are set forth in subsection (b)(2).

The type of electronic communication held by a remote computing service which is protected from governmental access is limited by certain preconditions. The communication must be on behalf of a subscriber or customer of a remote computing service and such communication must have been given to the remote computer service under narrow conditions. The narrow conditions are that the communication must have been received in a certain form (i.e. by means of electronic transmission or similar means). In addition, the communication must have been surrendered solely for the purpose of providing storage or computer processing services to the subscriber or customer, and the provider may not be authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Subsection (c) sets forth the rules under which the government may require the provider of electronic communications services or remote computing services to disclose a record or other transactional information concerning a subscriber or customer (other than the contents of a communication). The type of records involved are billing records and telephone toll records (including the record of long distance numbers and message unit detailing information). The government need not provide notice to the subscriber or customer before it seeks access to these types of records. On the other hand, the government must use one of three sets of authorized procedures. The government can rely on administrative subpoenas or grand jury subpoenas to the extent that such processes are legally authorized. Alternatively, the government can use a search warrant. Finally, the government can seek a court order directing the disclosure of such records. If a court order is sought then the government must meet the procedural requirements of subsection (d).

Subsection (d) provides that the government shows that there is reason to believe that the contents of an electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. The only contents which can be sought using the court order option are, of course, those stored for more than 180 days.

It should be noted that when the government is required to give notice to the customer or subscriber that the purpose of such notice is to provide the subscriber or customer with an opportunity to contest the propriety of such a disclosure. The customer or subscriber has standing to raise any legitimate defense to such disclosure including any constitutional claims under the First, Fourth, Fifth or Fourteenth Amendments, any claims of privilege, and any available defenses to improperly issued subpoenas. Whether any of these claims are accepted by the court before whom the application is pending will depend on the facts of a given case and the state of the law at the time.

Proposed section 2704 sets forth in four subsections the procedures governing back-up copy preservation.

Subsection (a)(1) provides that when the government is seeking access to remote computing service information on records under section 2703(b)(2) that the government can seek and obtain the assistance of the provider in preserving the information or records sought. The government may, under this subsection include with its subpoena or court order a request that the provider create or generate a back-up copy of the requested records or information. The provider is directed to create a back-up copy as soon as practicable consistent with its regular business practices. Thus, if a service promotor maintains back-up copies as part of its regular business activities, it does not have to create a new copy. The provider is directed not to inform the customer or subscriber of this activity. After the copy has been made the provider is directed to inform the governmental entity seeking the copy that it has complied with the request. Finally, this subsection sets as an outside limit for the creation of a back-up copy of two business days.

Subsection (a) provides that once the governmental entity has received confirmation that it shall notify the customer or subscriber within three days, unless such notice is delayed under the terms of proposed section 2704(c). At this point the provider is also free to notify the subscriber or customer unless prohited under subsection (b) of proposed section 2705

Subsection (a)(3) provides that the provider shall not destroy a back-up copy generated under this section until the latter of the delivery of the information or the resolution of any proceedings related to the access question. If the governmental entity has notified the customer or subscriber and that person has not challenged the requested access then after the passage of fourteen days the provider may make the disclosure. Subsection (a)(5) provides that a governmental entity may only seek to require the creation of a back-up copy under subsection (a)(1) if in its sole discretion there is reason to believe that notification under section 2703 may result in destruction or tampering with the information sought. This determination that notification under section 2703 may result in hampering with or destruction of evidence on similar adverse results by the governmental entity is not subject to challenge by the subscriber or customer or service provider.

Subsection (b)(1) of proposed section 2704 provides that within fourteen days after receipt of notice by the government that a back-up copy has been requested the subscriber or customer may move to quash or vacate. This subsection sets forth the procedural details of such proceedings. The challenger must service the governmental entity and provide written notice to the provider of the challenge. A motion to vacate shall be made in the court which issued the original order. Similarly, a motion to quash shall be made in the appropriate state or federal court. The motion or application under this subsection must establish that the challenger is the relevant customer or subscriber. The challenger must also set forth reasons why the records being sought are not relevant to a legitimate law enforcement inquiry or that some other legal defect exists such as failure by the government to comply with the requirements of this chapter.

Subsection (b)(2) sets forth service of process rules. Service under this section may be made by registered or certified mail to the appropriate governmental entity.

Subsection (b) provides that the government shall be directed to file a sworn response if the challenger has met the requirements of this subsection. The governmental response may be filed *in camera* if appropriate. If the court cannot on the basis of the initial set of papers determine the challenge, then additional proceedings may be conducted. Any additional proceedings and a decision on the challenge shall occur as rapidly as feasible, *i.e.* within 7 calendar days in all but the most unusual circumstances.

Subsection (b)(4) provides that if the court determines that the challenger is not the subscriber or the customer affected does not have legal standing to contest the disclosure then the court shall deny the motion or application. Denial is also directed if the court finds that the information sought is relevant to the legitimate law enforcement inquiry. On the other hand, if the challenger has standing and can show either lack of relevance or non-compliance with the procedural requirements of this section then the court may vacate the order or quash the subpoena.

In the event that there is no indictment then the person whose records are involved may move for the return of the records.

Subsection (b)(5) provides that a court order denying a motion or application under this section shall not be deemed a final order and therefore no interlocutory appeal may be taken from such a denial. Obviously, nothing precludes a customer or subscriber who is later the subject of a criminal proceeding from raising these issues again subject to the sanctions limitation of section 2708.

Proposed section 2705 (a) provides the conditions wherein delay of any required notification may be achieved. Under subsection (a)(1) a governmental entity may request a delay of notification for a period of up to 90 days if the governmental entity convinces the court that there is reason to believe that such notification will produce adverse results as described in subsection (a)(2) of proposed section 2704. Alternatively, where an administrative or grand jury subpoena is obtained, delay may be achieved if a supervisory official files a written certification that such delay is necessary to avoid adverse results. In the second case, the delay in notice can only last initially for a period of up to 90 days.

Subsection (a)(2) sets forth the adverse results which can trigger the delay of notification set out in paragraph (1) of this section. There are five enumerated adverse results: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses (including victims of any crimes); and (5) otherwise seriously jeopardizing an investigation or unduly delaying an ongoing trial.

Subsection (a)(3) requires the government to maintain a true copy of the certification required under paragraph (1)(B) of this section.

Subsection (a)(4) provides that extensions of up to 90 days may be made of the notification so long as the original requirements of this section are met with respect to the extension.

Subsection (a)(5) provides that upon the expiration of any period of delay the governmental entity which has obtained the information shall serve upon the customer or subscriber a copy of the process used to obtain the information. Service under this subsection can be by first class or registered mail. In addition, the government entity must also include a notice that states with reasonable specificity the nature of the law enforcement inquiry. Such notice shall also tell the customer or subscriber when the information was furnished, that the notification was delayed, who authorized the delay and under what provision of law.

Subsection (a)(6) defines, for purposes of this subsection, the term "supervisory official". Such term means the investigative agent or assistant investigative agent in charge or an equivalent official in the investigating agency's headquarters or regional office. The term also means the chief prosecuting attorney or first assistant prosecuting attorney or an equivalent official in a regional or headquarters office.

Subsection (b) of this section provides a procedure for the government to preclude the service provider from notifying the customer or subscriber in a narrow set of circumstances. First, such preclusion may only be obtained in instances where the government is not required to notify, or where the government has obtained the authority to delay notification. Second, a preclusion of notification must be granted by a court of competent jurisdiction. The final requirement is that the court be convinced that there is reason to believe that adverse results set forth in subsection (b) will occur if notification is given.

Sections 2702, 2703 and 2704 affect the contents of communications in storage or where information is being maintained for a subscriber or customer in a remote computing facility. New technologies have created capacities for storage of communications and the single prohibition of interception is not sufficient to cover this record-type aspect of communication. A person who subscribes to an electronic mail service may not realize it, but that service likely maintains a record of all system transactions for a period of time, usually six months under current industry practice. Even if the subscriber reads the message and discards or deletes it, the system maintains it as a backup copy for system maintenance and integrity purposes. These records are retrievable and the Committee intends that subscribers and customers be afforded some protection as to these records. Therefore, a provider of electronic communications to the public such as an electronic mail service may not disclose the contents of stored communications unless one of the statutory exceptions in 2702(b) apply. One of the exceptions, (b)(2), applies where the government has requested access either under section 2703 or 2516.

The Committee has sought to add significant protection to the provision of remote computing services where the contents of communications are electronically transmitted to such service. In most instances, records maintained by third parties have no special privacy or confidentiality protection. The United States Supreme Court has held that an employer's wage records are not subject to the assertion of interest by an employee. *Donaldson v. U.S.*, 400 U.S. 517 (1971). Similarly, in *Miller v. U.S.*, 425 U.S. 435, 1976, the

Court held that an individual has no standing to challenge the disclosure to government of records maintained by banks for their checking account customers. In *Donaldson*, the records sought were the wage records of the employer and were not kept or maintained for the employee. In *Miller*, the bank customer used the bank as an agent to facilitate financial transactions. The records of a checking account were evidence of a public transaction and the disclosure of them to a grand jury did not violate any constitutional rights of bank customers.

These cases were studied extensively by the United States Privacy Protection Study Commission and by the Congress. The Report of the Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977). The Privacy Commission recommended that individuals have enforceable rights to limit the disclosure of records maintained about them for third parties. The Congress acted upon these recommendations in the financial records area by enacting the Right to Financial Privacy Act in 1978. 12 U.S.C. 3400 et seq. That statute in overruling *Miller* requires federal government agencies to use legal process to obtain bank records and allow the bank customer to seek to quash such process.

Last term the Congress extended this type of record privacy protection to records maintained by cable operators. In the Cable Communications Privacy Act of 1984, cable companies in the provision of one-way and two-way services are restricted in the type of information they may disclose about subscribers. Public Law 98-549. Moreover, the legislation, like the Right to Financial Privacy Act, requires the government to obtain records only through a court order or legal process with an opportunity to the subscriber to appear and contest the disclosure of the information.

This Committee is convinced that the subscribers and customers of remote computing services should be afforded a level of confidence that the contents of records maintained on their behalf for the purpose of providing remote computing services will not be disclosed or obtained by the government, unless certain exceptions apply or if the government has used appropriate legal process with the subscribers or customers being given an opportunity to protect their rights.

Proposed section 2706 contains two subsections. Subsection (a) provides that a governmental entity obtaining the contents of communications, records or other transactional information under section 2702, 2703 (with certain exceptions) or 2704 of this title shall pay the person or entity providing such information a fee. The fee under this section shall be reimbursement for such costs as are reasonably necessary and which have been directly incurred in search for, assembly, reproducing or otherwise providing such information. Included in such costs are delivery costs. Also included are any costs due to the necessary disruption of the normal operations of a provider.

Subsection (a) exempts from the reimbursement provisions certain types of records unless the requirement of subsection (c) are met. The type of records involved are telephone toll records and telephone listings. These records are excluded, because for the most part the government has not traditionally paid for such information. Nothing in this exclusion, however, affects the government's obligation to pay for information through other requests (i.e. requests other than under this chapter). Thus, if a government agent uses a telephone to request information assistance then compensation will be due. Similarly any court appearances in connection with such an information request would be covered elsewhere.

Subsection (b) provides that the amount of the fee provided by subsection (a) of this section shall be either mutually agreed upon or determined by the appropriate court. The subsection specifies which court would be appropriate.

Subsection (c) of proposed section 2703 provides that a court may, upon the request of a person providing information, request an appropriate court to order reimbursement for payment related to expenses incurred in connection with the searching for, reproducing, or transporting books, papers, records, or other information or data required or requested to be produced. *See, e.g.*, 12 U.S.C. 3415. The provider may obtain such reimbursement if the information required is voluminous or otherwise causes an undue burden on the provider. The Committee expects that the Department of Justice will, by regulation (subject to notice and comment), promulgate written criteria to guide the parties and the courts with respect to the meaning of the terms "voluminous" and "undue burden". The Committee hopes that the uniform application of regulations will reduce the need to rely on judicial intervention to resolve reimbursement disputes. The most important factor to examine is the nature of current and past practice in this area. To the extent that the request exceeds the nature and scope of information usually sought without compensation then the reimbursement provisions would come into play.

Proposed Section 2707 contains five subsections. Subsection (a) provides a civil cause of action for any subscriber or customer who has been aggrieved by a knowing or intentional violation of this chapter. Recovery may be had under this section against a person or entity who violated the provisions of this chapter. This includes governmental entities who have violated the provisions of this chapter. Relief as may be appropriate may be awarded under this section but includes preliminary and other equitable relief, declaratory relief, damages and reasonable attorney's fees and other litigation costs reasonably incurred. Subsection (c) provides the measure of damages under this section. Damages include actual damages, any lost profits but in no case less than $1,000.

Subsection (d) sets forth defenses to civil actions. This subsection provides that good faith reliance on a lawful order shall be a complete defense to any civil or criminal action brought under this chapter or any other law. The types of lawful orders are set forth as (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization, (2) a request of any investigative or law enforcement officer under section 2518(7); or (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of.

Subsection (e) provides the statute of limitations. Under this subsection a civil action may not be commenced later than two years after the date upon which the claimant first discovered or had reasonable opportunity to discover the violation.

Proposed section 2708 provides that the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter. See discussion of section 101(e) of the bill, *supra*.

Proposed section 2709 contains provisions relating to counterintelligence access to telephone toll and transactional records. Subsection (a) provides that a communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information or electronic communication transactional records when such a request is made by the Director of the Federal Bureau of Investigation under subsection (b) of this section. Subsection (b) provides that the Director of the FBI (or an individual within the FBI designated for that purpose by the Director) may request any such information and records if there is a certification that the information sought is relevant to an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power (as those terms are defined in the Foreign Intelligence Surveillance Act of 1978).

Subsection (c) provides that a communications common carrier or service provider (including officers, employees and agents) shall not disclose to any person that the FBI has sought or obtained such information or records.

Subsection (d) provides that the FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign counterintelligence collection and foreign counterintelligence investigations conducted by the FBI, with respect to dissemination to an agency of the United States. Any disclosure to a United States agency can only be made if the information is clearly relevant to the authorized responsibilities of such agency.

Subsection (e) provides that the Director of the FBI shall fully inform the House and Senate intelligence committees concerning all requests made under this section.

Proposed section 2910 contains definitions used in this chapter. As a general rule, the terms used in this new chapter have the same definitions as such terms have when used in chapter 119. The term "remote computing service" means "the provision to the public of computer storage or processing services by means of any electronic communication system." Remote computing services is not intended to apply to computer services offered by the various telephone company central offices in connection with the routing of telephone calls (such as speed dialing, call forwarding, and three-way dialing). Computer storage means all types of electronic or magnetic storage, including storage in the memory of a computer.

Section 201(b) contains a clerical amendment to amend the table of chapters to add a new title for chapter 121.

Section 202 of the bill contains the effective date. For this title and the amendments made by this title, the effective date is 90 days after the date of enactment. In the case of conduct pursuant to a court order or extension, it will apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

This title contains one section and two subsections of the bill. Section 301(a) adds six new sections to title 18 relating to pen registers.

Proposed section 3121 contains three subsections. Subsection (a) contains a general prohibition on pen register use. The subsection provides that no person shall install or use a pen register without first obtaining a court order under section 3123 or under the Foreign Intelligence Surveillance Act.

Subsection (b) contains exceptions to the general list of prohibitions. The subsection provides that the prohibitions do not apply with respect to the use of a pen register by a provider of electronic or wire communication service if either of two conditions are met. The first condition is that such use relates to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of the service or unlawful use of service.

The second permissible condition for the use of a pen register is to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

Subsection (c) provides that penalty for knowingly violating subsection (a). The penalty is a fine under this title or imprisonment of up to one year, or both.

The absence of any specific civil cause of action for violations of proposed chapter 206 was purposeful; therefore, no private cause of action should be implied under this chapter.

Proposed section 3122 provides the procedures for making an application for a pen register order. Under subsection (a) an attorney for the government may make an application for an order or an extension of an order authorizing or approving the installation and use of pen registers. The application shall be in writing under oath or equivalent affirmation to a court of competent jurisdiction. Subsection (a)(2) contains parallel provisions with respect to state applications. The phrase ". . . unless otherwise prohibited by State law" in this subsection makes clear that this law does not preempt any existing state laws with respect to installation and use of pen registers by state officials. To the extent that state law currently provides that a pen register may only be installed or used by a state official based on some other, higher standard of proof, that law will continue in effect with respect to such officials. *See People* v. *Sporleder*, 666 P. 2d 135 (Colo. Sup. Ct. 1983); Note, On Privacy, Pen Registers, and State Constitutions: The Colorado Supreme Court Rejects *Smith* v. *Maryland*, 15 Tol L. Rev. 1466 (1984); *People* v. *McCunes*, 51 Cal. App. 3d 487 (1975). Subsection (b) provides what factual details need to be provided in the application. The application shall include the identity of the attorney for the federal or state government and the identity of the applicant making the application, and a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

Proposed section 3123 contains four subsections. Subsection (a) provides that upon an application the court shall issue an *ex parte* order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the government attorney has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. This provision does not envision an independent judicial review of whether the application meets the relevance standard rather the court needs only to review the completeness of the submitted certification.

Subsection (b) sets forth the contents of the order for a pen register, authorization or installation. The order is required to specify (1) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is attached; (2) the identity, if known, of the person who is the subject of the criminal investigation; (3) the number and, if known, physical location of the telephone line to which the pen register is attached; and (4) a statement of the offense to which the information likely to be obtained by the pen register relates. In addition, the order shall direct, upon request, the furnishing of information facilities and technical assistance necessary to accomplish the installation of the pen register. The content of the order relating to cooperation is intended to codify the existing informal practice of cooperation between the telephone companies and the Department of Justice.

Subsection (c) provides that the time period of authorization of an installation and use of a pen register is 60 days, with possible extensions of 60 days.

Subsection (d) provides that an order authorizing or approving the installation and use of a pen register shall direct that the order be sealed, until otherwise ordered by the court. In addition, the order shall bar the disclosure of the existence of a pen register or an investigation to the listed subscriber, or to any other unauthorized person, unless or until otherwise directed by the court. Intentional violations of the non-disclosure provisions may be, in appropriate circumstances, punishable as contempt.

Proposed section 3124 contains two subsections. Subsection (a) provides that upon the request of an authorized person a provider of a wire communication service, landlord, custodian, or other person shall furnish such person with all information, facilities, and technical assistance necessary to effectuate the order unobtrusively and with a minimum of interference. The Committee assumes that the current practice of law enforcement officials installing and maintaining the pen register will continue. Subsection (b) provides that the persons giving assistance under this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance. This compensation provision is modeled after that which applies under chapter 119 of title 18 and is intended to be interpreted and implemented in a similar fashion.

Proposed section 3125 provides that the Attorney General shall annually report to the Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice. Under a current order of the Attorney General statistics concerning pen registers are compiled. Memorandum from Assistant Attorney General, Criminal Division, Department of Justice, Phillip B. Heyman to all Investigative Agencies, dated Sept. 24, 1979 (Recording the number of investigations, number of persons affected and nature of the offenses). This section merely requires that this information be reformulated and submitted to the appropriate committees of the Congress. Obviously the greater the detail contained in these reports the less need there will be for supplemental activities. Therefore, it would be helpful to the Committee if these reports could indicate for which offenses pen registers are being used.

Proposed section 3126 contains definitions for this chapter. Subsection (a) contains the definitions. The term "communications common carrier" has the same meaning as is found in section 3(h) of the Communications Act of 1934. The term "wire communication" has the meaning set forth in section 2510 of this title. The term "court of competent jurisdiction" means a district court of the United States (including a magistrate of such court) or a United States Court of Appeals or a court of general jurisdiction of a State authorized to enter orders authorizing the use and installation of pen registers. The term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached. The term does not include the contents of a communication, rather it records the numbers dialed. Such term does not include any device used by a provider of wire communication service for billing, or recording as incident to billing, for communications services provided by such provider. The term "attorney for the government" has the meaning given to that term by the Federal Rules of Criminal Procedure. The term "state" means a State, the District of Columbia, Puerto Rico, and other possession or territory of the United States.

Subsection (b) of this section contains a clerical amendment amending the table of chapters.

Section 302 contains the effective date. Subsection (a) provides that as a general rule the amendments made by this title shall take effect 90 days after enactment. In addition, in the case of conduct pursuant to a court order or extension, these amendments apply only with respect to court orders or extensions made after the title takes effect.

Subsection (b) contains special rules or exceptions. This subsection, in essence, gives states two years to bring their laws into conformity with these amendments to federal law.

NEW BUDGET AUTHORITY

In regard to clause (l)(3)(B) of rule XI of the Rules of the House of Representatives, the bill creates no new budget authority or increased tax expenditures for the Federal judiciary.

INFLATIONARY IMPACT STATEMENT

In regard to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the commitee feels that the bill will have no foreseeable inflationary impact on prices or costs in the operation of the national economy.

FEDERAL ADVISORY COMMITTEE ACT OF 1972

The Committee finds that this legislation does not create any new advisory committees within the meaning of the Federal Advisory Committee Act of 1972.

COST ESTIMATE

In compliance with clause 7 of rule XIII of the Rules of the House of Representatives, the committee estimates that the costs which will be incurred in carrying out the provisions of the reported bill are accurately reflected in the Congressional Budget Office estimate.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 18, 1986.

Hon. PETER W. RODINO, Jr.,
Chairman, Committee on the Judiciary, House of Representatives,
Rayburn Office Building, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has reviewed H.R. 4952, the Electric Communications Privacy Act of 1986, as ordered reported by the House Committee on the Judiciary, June 10, 1986. CBO estimates that enactment of this legislation will result in no significant cost to the federal government and no cost to state or local governments.

H.R. 4952 makes a number of amendments to Title 18 of the United States Code concerning access to electronic communications. Title I of the bill establishes penalties for the unlawful interception or disclosure of electronic communications, provides for the recovery of civil damages for persons whose communications are intercepted, disclosed or used in violation of this provision, and modifies procedures for government interception of communications. Title II creates specific penalties for unlawful access to stored wire and electronic communications, while Title III establishes a general prohibition on the use of pen registers. These titles include specific procedures for access to stored communications and use of pen registers by government entities, and Title II includes a provision for civil actions.

H.R. 4952 requires government entities to compensate private parties assembling or providing information concerning stored electronic communications, or assisting in the installation and use of a pen register. Because such compensation is currently provided in Department of Justice investigations, CBO does not expect these provisions to involve any significant additional cost for the federal government.

Based on information from the Department of Justice, we do not expect enactment of this bill to result in a significant change in the government's law enforcement practices or expenditures. H.R. 4952 would provide a specific foundation in the code for current law enforcement efforts the Department is undertaking under other authority.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,

Sincerely,

RUDOLPH G. PENNER, *Director.*

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

PART I—CRIMES

Sec.

General provisions 1

* * * * * * *

119. Wire *and electronic communications* interception and interception of oral communications 2510

* * * * * * *

121. Stored Wire and Electronic Communications and Transactional Records Access 2701

* * * * * * *

CHAPTER 109—SEARCHES AND SEIZURES

* * * * * * *

§ 2232. Destruction or removal of property to prevent seizure

(a) PHYSICAL INTERFERENCE WITH SEARCH.—Whoever, before, during, or after seizure of any property by any person authorized to make searches and seizures, in order to prevent the seizure or securing of any goods, wares, or merchandise by such person, staves, breaks, throws overboard, destroys, or removes the same, shall be fined not more than $10,000 or imprisoned more than five years, or both.

(b) NOTICE OF SEARCH.—Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise or other property, gives notice or attempts to give notice of the possible search or seizure to any person shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement

officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.

* * * * * * *

CHAPTER 119—WIRE *AND ELECTRONIC COMMUNICATIONS* INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.
2510. Definitions.

* * * * * * *

2521. Injunction against illegal interception.

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any [communication] *aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception *(including the use of such connection in a switching station)* furnished or operated by any person engaged [as a common carrier] in providing or operating such facilities for the transmission of interstate or foreign communications *or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;*

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, *but such term does not include any electronic communication;*

* * * * * * *

(4) "intercept" means the aural *or other* acquisition of the contents of any wire, *electronic,* or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire [or oral], *oral, or electronic* communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a [communications common carrier] *provider of wire or electronic communication service* in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

* * * * * * *

(8) "contents", when used with respect to any wire [or oral], *oral, or electronic* communication, includes any information concerning the [identity of the parties to such communication or the existence,] substance, purport, or meaning of that communication;

(9) "Judge of competent jursidiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire [or oral], *oral, or electronic* communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; [and]

(11) "aggrieved person" means a person who was a party to any intercepted wire [or oral], *oral, or electronic* communication or a person against whom the interception was direct*ed*[.]*;*

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title);

(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider or such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

§ 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire [or oral] *oral, or electronic* communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the permises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; or

(d) willfully uses, or endeavors to use, the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; [shall be fined not more than $10,000 or imprisoned not more than five years, or both.] *shall be punished as provided in subsection (4).*

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of [any communication common carrier,] *a provider of wire or electronic communication service,* whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property [of the carrier of such communication: *Provided,* That said communication common carriers] *of the provider of that service, except that a provider of wire communication service to the public* shall not utilize service observing or random monitoring except for mechanical or service qualtiy control checks.

(ii) Notwithstanding any other law, *providers of wire or electronic communication service,* [communication common carriers,]their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information facilities, or technical assistance to persons authorized by law to intercept wire [or oral] , *oral, or electronic* communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if [the common carrier,] *such provider* its officers, employees, or agents, landlord, custodian, or other specified person has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No [communication common carrier] *provider of wire or* *electronic communication service* officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any violation of this subparagraph by a [communication common carrier] *provider of wire or electronic communication service* or an officer, employee, or agent thereof, shall render the carrier liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any [communication common carrier] *provider of wire or electronic communication service* its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire *or electronic* communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire [or oral], *oral, or electronic* communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire [or oral], *oral, or electronic* communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the pupose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State [or for the purpose of committing any other injurious act].

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an office, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter *or chapter 121,* or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communication [by], *or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing* a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress:

(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register (as that term is defined for the purpose of chapter 206 (relating to pen registers) of this title);

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted.

(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof)

while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(B) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who willfully—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire **[**or oral**]**, *oral, or electronic* communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire **[**or oral**]**, *oral, or electronic* communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) **[**a communications common carrier**]** *a provider of wire or electronic communication service* or an officer, agent, or employee of, or a person under contract with, **[**a communications common carrier**]** *such a provider,* in the normal course of the **[**communications common carrier's business**]** *business of providing that wire or electronic communication service,* or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire **[**or oral**]**, *oral, or electronic* communications.

§ 2513. Confiscation of wire [or oral], *oral, or electronic* communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

§ 2515. Prohibition of use as evidence of intercepted wire [or oral], *oral, or electronic* communications

Whenever any wire [or oral], *oral, or electronic* communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire [or oral], *oral, or electronic* communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, [or] any Assistant Attorney General, *any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division* specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), *section 751 (relating to escape),* sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), *section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity),* section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 2252 or 2253 (sexual exploitation of children), sections 2251 and 2252 (sexual exploitation of children), sections [2314] *2312, 2313, 2314,* and 2315 (interstate transportation of stolen property), *the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities),* section 1963 (violations with respect to racketeer influenced and corrupt organizations), *section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud),* or section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassination, kidnapping, and assault);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions); [or]

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain devices) of this title;

(i) the location of any fugitive from justice from an offense described in this section; or

[(h)]*(j)* any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire [or oral], *oral, or electronic* communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire [or oral], *oral, or electronic* communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or deal-

ing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§ 2517. Authorization for disclosure and use of intercepted wire **[**or oral**]**, *oral, or electronic* communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire **[**or oral**]**, *oral, or electronic* communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire **[**or oral**]**, *oral, or electronic* communication or evidence derived therefrom any use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire **[**or oral**]**, *oral, or electronic* communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire **[**or oral**]**, *oral, or electronic* communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire **[**or oral**]**, *oral, or electronic* communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. Procedure for interception of wire [or oral], *oral, or electronic* communications

(1) Each application for an order authorizing or approving the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) *except as provided in subsection (11),* a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatially terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire [or oral], *oral, or electronic* communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving inteception of wire [or oral], *oral, or electronic* communications within the territorial jurisdiction of the court in which the judge is sitting *(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction) after within the territorial jurisdiction of the*

court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter.

(b) there is probable cause for brief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) *except as provided in subsection (11),* there is probable cause for belief that the facilities from which, or the place where, the wire [or oral], *oral, or electronic* communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire [or oral], *oral, or electronic* communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall, upon request of the applicant, direct that a [communication common carrier,] *provider of electronic communication service,* landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant [at the prevailing rates.] *for reasonable expenses incurred in providing such facilities or assistance.*

(5) No order entered under this section may authorize or approve the interception of any wire [or oral], *oral, or electronic* communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. *Such thirty-day period begins on the earlier of the day on which the*

investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise, subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. *In the event the intercepted communications is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.*

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person.

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire [or oral], *oral, or electronic* communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire [or oral], *oral, or electronic* communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire [or oral], *oral, or electronic* communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire [or oral], *oral, or electronic* communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire [or oral], *oral, or electronic* communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under this directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire [or oral], *oral, or electronic* communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire [or oral], *oral, or electronic* communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(i) in the case of an application with respect to the interception of an oral communication—

(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General,

the Deputy Attorney General, the Associate Attorney General an Assistant Attorney General, or an acting Assistant Attorney General;

(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(III) the judge finds that such specification is not practical; and

(ii) in the case of an application with respect to a wire or electronic communication—

(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

(III) the judge finds that such purpose has been adequately shown.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.

§2519. Reports concerning intercepted wire [or oral], *oral, or electronic* communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for *(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)*;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension or an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or

the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire **[**or oral**]**, *oral, or electronic* communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

[Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to interecept, disclose, or use such communications, and (2) be entitled to recover from any such person—

[(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

[(b) punitive damages; and

[(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.]

§ 2520. Recovery of civil damages authorized

(a) In General.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief.—In an action under this section appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropariate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages.—The court may assess as damages in an action under this section whichever is the greater of—

(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determiniation of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

Sec.
2701. Unlawful access to stored communications.
2702. Disclosure of contents.
2703. Requirements for governmental access.
2704. Backup preservation.
2705. Delayed notice.
2706. Cost reimbursement.
2707. Civil action.
2708. Exclusivity of remedies.
2709. Counterintelligence access to telephone toll and transactional records.
2710. Definitions.

§ 2701. Unlawful access to stored communications

(a) Offense.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communications while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703 or 2704 of this title.

§ 2702. Disclosure of contents

(a) Prohibitions.—Except as provided in subsection (b)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity

the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) to a law enforcement agency, if such contents—

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime.

§ 2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscribe or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communications Service or Remote Computing Service.—A governmental entity may require a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(3) obtains a court order for such disclosure under subsection (d) of this section.

(d) Requirements for Court Order.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

§ 2704. Backup preservation

(a) Backup Preservation.—(1) A governmental entity acting uinder section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subcriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicalbe consistent with its regular business practices and shall confirm to the governmental entrity that such backup copy has been

made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of—

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the government entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determiantion is not subject to challenge by the subscriber or customer or service provider.

(b) CUSTOMER CHALLENGES.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district or State court. Such motion or application shall contain an affidavit or sworn statement—

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer had complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the rea-

sons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or applications decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§ 2705. Delayed notice

(a) Delay of Notification.—(1) A governmental entity acting under section 2703(b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days; if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse resut for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application,

or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customers or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" mans the investigtive agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 2706. Cost reimbursement

(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such infor-

mation. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil Action

(a) Cause of Action.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (3); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

(d) Defense.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(e) Limitation.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

§ 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to Provide.—A Communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required Certification.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(c) Prohibition of Certain Disclosure.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by Bureau.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement That Certain Congressional Bodies Be Informed.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

§ 2710. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.

PART II—CRIMINAL PROCEDURE

Chap. Sec.
201. General provisions 3001

* * * * * * *

206. Pen Registers 3121

* * * * * * *

CHAPTER 205—SEARCHES AND SEIZURES

Sec.
3101. Effect of rules of court—Rules.

* * * * * * *

3117. Moble tracking devices.

* * * * * * *

§ 3117. Mobile tracking devices

(a) In General.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) Definition.—As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

CHAPTER 206—PEN REGISTERS

Sec.
3121. General prohibition on pen register use; exception.
3122. Application for an order for a pen register.
3123. Issuance of an order for a pen register.
3124. Assistance in installation and use of a pen register.
3125. Reports concerning pen registers.

§ 3121. General prohibition on pen register use; exception

(a) In General.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent or the user of that service.

(c) Penalty.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122. Application for an order for a pen register

(a) Application.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of Application.—An application under subsection (a) of this section shall include—

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3123. Issuance of an order for a pen register

(a) In General.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(b) Contents of Order.—An order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

(c) Time Period and Extensions.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon

the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

(d) Nondisclosure of Existence of Pen Register.—*An order authorizing or approving the installation and use of a pen register shall direct that—*

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register

(a) In General.—*Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.*

(b) Compensation.—*A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.*

§ 3125. Reports concerning pen registers

The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

§ 3126. Definitions for chapter

As used in this chapter—

(1) the term "communications common carrier" has the meaning set forth for the term "common carrier" in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

(2) the term "wire communication" has the meaning set forth for such term in section 2510 of this title;

(3) the term "court of competent jurisdiction" means—

(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

(4) the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communi-

cations, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

* * * * * * *

○